INFORMATION HIDING
AN ANNOTATED BIBLIOGRAPHY

Ross J. Anderson and Fabien A. P. Petitcolas

Computer Laboratory
University of Cambridge
Cambridge CB2 3QG, UK

There are a number of application areas in which we want to hide information or to stop someone else from doing so. These include steganography, copyright marking, the study of covert channels in operating systems, low-probability-of-intercept communications, and the study of subliminal channels in digital signature schemes.

There follow abstracts of material from number of relevant publications. A six digit number (e.g. 034412) is an abstract number in 'Computer and Communications Security Reviews': see `http://www.anbar.co.uk/computing/ccsr/` for copies of this journal.

Version: $Id: bibliography.tex,v 1.25 1999-08-13 08:33:40+01 fapp2 Exp $
The electronic version of this document is available at:
`http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/`

Contents

Form SF298 Citation Data

Report Date ("DD MON YYYY") 13041999	Report Type N/A	Dates Covered (from... to) ("DD MON YYYY")

Title and Subtitle Information Hiding an Annotated Bibliography	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 63	

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	4/13/99	Report

4. TITLE AND SUBTITLE
Information Hiding an Annotated Bibliography

5. FUNDING NUMBERS

6. AUTHOR(S)
Not provided

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Information Assurance
Technology Analysis Center
(IATAC)
3190 Fairview Park Drive
Falls Church, VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical
Information Center
DTIC-AI
8725 John J. Kingman Road,
Suite 944

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

There are a number of application areas in which we want to hide information or to stop someone else from doing so. These include steganography, copyright marking, the study of covert channels in operating systems, low-probability of intercept communications, and the study of subliminal channels in digital signature schemes. There follow abstracts of material from number of relevant publications. A six digit number (e.g. 034412) is an abstract number in 'Computer and Communications Security Reviews': see http://www.anbar.co.uk/computing/ccsr/ for copies of this journal.

14. SUBJECT TERMS
Cryptography, Information Hiding,

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Unlimited

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

1 New

[1] **'Transform Permuted Watermarking for Copyright Protection of Digital Video'**
A. Johnson, M. Biggar, in Globecom 98, Sydney, Australia, 8–12 Nov. 1998.
The paper briefly reviews watermarking approaches for digital video and proposes a new transform domain technique that uses data randomisation prior to the insertion of a mark which involves the modification of selected transform coefficients. The implementation results shows successful recovery of the mark and robustness of the scheme against digital to analogue and analogue to digital conversion.

[2] **'The business case for audio watermarking'**
P. Jessop, International Conference on Acoustics, Speech and Signal Processing [80], pp. 2077–2080.
The paper examines the reasons for inserting digital watermarks in sound recordings, the benefits and issues which might result.

[3] **'If one watermark is good, are more better?'**
F. Mintzer, G. W. Braudaway, International Conference on Acoustics, Speech and Signal Processing [80], pp. 2067–2070.
The author discusses the issues involved when embedding multiple watermarks of different or similar types. The order in which the marks are applied is very important. Strong watermarks should be embedded first and fragile watermarks last. Watermark of the same type should be embedded simultaneously.

[4] **'Detecting electronic watermarks in digital video'**
J.-P. M. G. Linnartz, T. Kalker, J. Haitsma, International Conference on Acoustics, Speech and Signal Processing [80], pp. 2071–2074.
The authors extend their previous work ([363, 267]) by proposing a model to evaluate the effect of scaling on the mark detector reliability. The model is then verified with experiments.

[5] **'Circularly symmetric watermark embedding in 2-D DFT domain'**
V. Solachidis, I. Pitas, International Conference on Acoustics, Speech and Signal Processing [80], pp. 1653–1656.

The authors propose a watermarking method robust to rotation and scaling. The watermark is circular and composed of S sectors. It is added directly to the DFT of the original image, and no visual model is used. The original is not required for detection, which tells simply whether a suspect image contains a mark or not.

[6] **'An Introduction to Watermark Recovery from Images'**
N. F. Johnson, in Conference and Workshop on Intrusion Detection and Response (IDR'99), San Diego, California, U.S.A., 9–13 Feb. 1999, System Administration Networking Security Institute, pp. 10–A1–10–A6.
The author discusses a method of recovering digital watermarks in images after StirMark attack.

[7] **'Storage and Retrieval for Image and Video Database V'**
I. K. Sethin, R. C. Jain, Eds., vol. 3022, San Jose, California, U.S.A., Feb. 1997. The Society for Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIE), SPIE. ISBN 0-8194-2433-1, ISSN 0277-786X.

[8] **'Robust Labeling Methods for Copy Protection of Images'**
G. C. Langelaar, J. C. A. van der Lubbe, R. L. Lagendijk, in Sethin, Jain [271], pp. 298–309.
The authors present two labeling techniques for images.The first divides the image into blocks and apply a variant of Pitas' method [134] using JPEG compression as feedback to each of them. The second removes certain high frequency D.C.T.-coefficients to embed the label.

[9] **'A watermark for digital images'**
R. B. Wolfgang, E. J. Delp, in International Conference on Images Processing, Lausanne, Switzerland, 16–19 Sept. 1996, IEEE, pp. 219–222.
The authors present a technique based on D.S.S. A PN-Sequence is added to the image. The two-dimensional approach helps to detect where the image has been forged. The watermark survives JPEG compression to a certain extent.
`<http://dynamo.ecn.purdue.edu/˜ace/delp-pub.html##VidSecure>`.

[10] **'Security and Watermarking of Multimedia Contents'**
P. W. Wong, E. J. Delp, Eds., vol. 3657, San Jose, California, U.S.A., 25–27 Jan. 1999. The Society for Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIE), SPIE. ISBN 0-8194-3128-1, ISSN 0277-786X.

[11] **'Broadcast monitoring: a practical application of audio watermarking'**
D. Blagden, N. Johnson, Announced for publication in [10] but withdrawn. Presented at the conference.
The authors present the AudioTag system which adds a watermark into broadcast material to allow monitoring.

[12] **'Selective assignment approach for robust digital image watermarking'**
K. S. Ng, L. M. Cheng, in Wong, Delp [10], pp. 13–20.
The authors present a block based watermarking algorithm for digital images. The D.C.T. of the block is increased by a certain value. Quality control is done using SNR. Only robustness to JPEG is considered.

[13] **'Secure Robust Digital Watermarking Using the Lapped Orthogonal Transform'**
S. Pereira, J. J. K. Ó Ruanaidh, T. Pun, in Wong, Delp [10], pp. 21–30.
The us of small block to embed watermarks facilitate the use of adaptive models based on the human vision system. However, blocking introduces artefacts at the borders between blocks. The authors suggest to use the lapped orthogonal transform to circumvent this. Robustness to general linear geometrical transformations is tackled by using an invisible template.
`<http://cuiwww.unige.ch/˜vision/Publications/postscript/99/PereiraORuanaidhPun_eiswmc99.ps.gz>`.

[14] **'A DWT-based technique for spatio-frequency masking of digital signatures'**
M. Barni, F. Bartolini, V. Cappellini, A. Lippi, A. Piva, in Wong, Delp [10], pp. 31–39.
The authors present a public watermarking system. A binary pseudo random sequence is weighted with a function, which takes into account the human visual system (orientation brightness, texture) and then added to the wavelet transform of an image. The detection tells whether the watermark is present or not. Robustness to JPEG compression, median filtering, multiple watermarking and cropping is considered.
<http://lci.die.unifi.it/Publications/swmc99-04.ps.gz>.

[15] **'Perceptual Watermarks for Digital Images and Video'**
R. B. Wolfgang, C. I. Podilchuk, E. J. Delp, in Wong, Delp [10], pp. 40–51.
The authors review some watermarking techniques that use perceptual models to produce invisible yet robust watermarks.
<ftp://skynet.ecn.purdue.edu/pub/dist/delp/ei99-water/>.

[16] **'Issues for Authenticating MPEG video'**
C.-Y. Lin, S.-F. Chang, in Wong, Delp [10], pp. 54–65.
This is an enhanced version of (**074144**). The authors first discuss MPEG video authentication under various transcoding situations (including dynamic rate shaping, requantization, frame type conversion and re-encoding) and propose a system that tolerate some of them.
<http://www.ctr.columbia.edu/~cylin/pub/spie99paper.ps>.

[17] **'Verification Watermarks on Fingerprint Recognition and Retrieval'**
S. Pankanti, M. M. Yeung, in Wong, Delp [10], pp. 66–78.
The authors are concerned about the impact of image watermarking on automatic processing of these images such as feature extraction and recognition techniques. They focus on human fingerprint recognition and demonstrate that there is no significant statistical deviation.

[18] **'Fragile imperceptible digital watermark with privacy control'**
D. Coppersmith, F. Mintzer, C. Tresser, C. W. Wu, M. M. Yeung, in Wong, Delp [10], pp. 79–84.
The authors propose a system to authenticate images by an authentication agent without revealing the human-readable content of the image to the agent. The most significant bits are signed and the signature together with name of the owner and privacy enhanced data are placed into the least significant bit plane in a similar way to Walton (**1054**).

[19] **'Content-based integrity protection of digital images'**
M. P. Quelez, in Wong, Delp [10], pp. 85–93.
The author present a framework for image authentication and a method to embed fragile watermarks into images and videos. Robustness to JPEG and MPEG2 compression and sensitivity to manipulation are evaluated.

[20] **'Exploring CDMA for watermarking of digital video'**
B. G. Mobasseri, in Wong, Delp [10], pp. 96–102.
The authors agues that spread-spectrum in the form of code division multiple access is more suitable for digital watermarking than other variant of spread spectrum. The system based on CDMA is proposed and shown to be robust to noise addition and de-synchronisation such as frame removal.

[21] **'A video watermarking system for broadcast monitoring'**
T. Kalker, G. Depovere, J. Haitsma, M. Maes, in Wong, Delp [10], pp. 103–112.
The authors describe a system for monitoring broadcast video developed in the context of the European ESPRIT project VIVA. It is based on a invisible watermarking system which is robust to all processing steps involved in broadcasting,

has a low probability of false alarm and allows low complexity real-time detection. Information is embedded by using the relative position of hidden signals.
<http://www-wavelet.eecs.berkeley.edu/˜kalker/Papers/spie99/spie99.pdf>.

[22] **'Robust 3D DFT video watermarking'**
F. Deguillaume, G. Csurka, J. J. K. Ó Ruanaidh, T. Pun, in Wong, Delp [10], pp. 113–124.
In contrast to previous work on video watermarking, the authors propose to watermark three dimensional chunks of video scene (spatial and time). As in their previous work on still image watermarking, the authors embed both a watermark and a template to facilitate recovery and use a 3D log map to survive rotation and scaling. Robustness to compression, resynchronisation, aspect-ratio, frame-rate changes and combination of them are considered.
<http://cuiwww.unige.ch/˜vision/Publications/postscript/99/DeguillaumeCsurkaORuanaidhPun_eiswmc99.ps.gz>.

[23] **'IPR techniques applied to a multimedia environment in the HYPERMEDIA project'**
A. M. noz, A. Ribagorda, J. M. Sierra, in Wong, Delp [10], pp. 125–132.
The author evaluate the robustness of Cox's algorithm to collusion attack.
<http://benjusuf.uc3m.es/alberto/SPIE99-1.zip>.

[24] **'Watermark estimation through local pixel estimation'**
M. Holliman, N. Memon, M. M. Yeung, in Wong, Delp [10], pp. 134–146.
The authors describe a method by which an attacker can attempt to construct an approximation to the watermark by taking advantage of inter-pixel correlation. The attack is applicable to watermarking techniques based on the addition of a pseudo-noise signal taking values into $-1, 1$ to an image. The sign of a watermark element $W_{x,y}$ at location (x, y) is estimated by comparing a pixel to its neighbourhood average: $\hat{s}_{x,y} = \mathrm{sign}(\tilde{I}_{x,y} - \sum_{(m,n)\in P_{x,y}} \alpha_{m,n}\tilde{I}_{x+m,y+n})$.

[25] **'Spread Spectrum Watermarking: Malicious Attacks and Counterattacks'**
F. Hartung, J. K. Su, B. Girod, in Wong, Delp [10], pp. 147–158.
The authors review and classify proposed attacks on spread spectrum watermarks and show how existing spread-spectrum based system can be improved by adapting the power of the watermark to the power of the host signal and using a block-wise multi-dimensional sliding correlator based watermark detector. The latter increases robustness to geometric distortions.
<http://www-nt.e-technik.uni-erlangen.de/˜hartung/publications/attacks.ps.gz>.

[26] **'A Channel Model for a Watermark Attack'**
J. K. Su, F. Hartung, B. Girod, in Wong, Delp [10], pp. 159–170.
The authors focus on sample reordering as a means for attacking spread-spectrum based watermarking systems. The reordering used here is shown to behave like a non-causal linear filter on average and the optimal detector is derived. The attack also applied to the multidimensional blockwise sliding correlator proposed in [25].
<http://www.nt.e-technik.uni-erlangen.de/˜su/downloads/ei99.ps.gz>.

[27] **'Combining digital Watermarks and collusion secure Fingerprints for digital Images'**
J. Dittmann, A. Behr, M. Stabenau, P. Schmitt, J. Schwenk, J. Ueberberg, in Wong, Delp [10], pp. 171–182.
The authors present a fingerprinting system robust to collusion of d persons in a set of q customers using fingerprints of length $n = \sum_{k=0}^{d} q^k$. The fingerprinting generation is based on dual rational normal curves. The embedding is done by adding the watermark to low frequencies of the D.C.T. matrix.

[28] **'Text-indicated speaker verification method using PSI-CELP parameters'**
T. Mogaki, N. Komatsu, H. Nishikawa, in Wong, Delp [10], pp. 184–193.
A method to verify the identity of mobile communication systems is proposed. It utilises the pitch synchronous innovation code excited linear prediction parameters. After giving his ID the user is challenged with a text to pronounce. The system verifies that the pronounced text is the right one and that the CELP parameters correspond to the right person. Results show that the systems works better for males than females.

[29] **'Non-Invertible Watermarking Methods FOR MPEG Encoded Audio'**
L. Qiao, K. Nahrstedt, in Wong, Delp [10], pp. 194–202.
This is a conference version of (**074150**).

[30] **'Fragile Watermarking Using the VW2D Watermark'**
R. B. Wolfgang, E. J. Delp, in Wong, Delp [10], pp. 204–213.
The authors show how hash functions can be used to identify and localise changes in images. A first method keeps the hashes of the column and rows of the picture but can only localise a single pixel modification without ambiguity. Another method uses block based has function. In this case the precision of the localisation is limited to the blocks. The authors also propose a better solution using a variable watermark two dimensional algorithm described in [9].
`<ftp://skynet.ecn.purdue.edu/pub/dist/delp/ei99-hash/>`.

[31] **'Comparing Robustness of Watermarking Techniques'**
J. Fridrich, M. Goljan, in Wong, Delp [10], pp. 214–225.
The authors propose a methodology for comparing robustness of watermarking techniques. Two variants are suggested: one for yes/no watermarking systems and the other for general public marking algorithms. A method to convert a multiple-bit technique into a one-bit technique and vice versa.
`<http://ssie.binghamton.edu/~jirif/Research/spie99.doc>`.

[32] **'A fair benchmark for image watermarking systems'**
M. Kutter, F. A. P. Petitcolas, in Wong, Delp [10], pp. 226–239.
The authors present an evaluation procedure of image watermarking systems. First they identify all necessary parameters for proper benchmarking and investigate how to quantitatively describe the image degradation introduced by the watermarking process. For this, they show the weaknesses of usual image quality measures in the context watermarking and propose a novel measure adapted to the human visual system. Then they show how to efficiently evaluate the watermark performance in such a way that fair comparisons between different methods are possible. Finally they review a number of attacks that any system should survive to be really useful and propose a benchmark and a set of different suitable images.
`<http://www.cl.cam.ac.uk/~fapp2/papers/ei99-benchmark/>`.

[33] **'OCTALIS benchmarking: Comparison of four watermarking techniques'**
L. Piron, M. Arnold, M. Kutter, W. Funk, J. M. Boucqueau, F. Craven, in Wong, Delp [10], pp. 240–250.
The benchmark includes evaluation of the watermark robustness and the subjective visual image quality. Two algorithms use the frequency domain while the two others use the spatial domain for watermarking. The tests show that no method survives geometrical transformations.

[34] **'Watermarking by histogram specification'**
D. Coltuc, P. Bolon, in Wong, Delp [10], pp. 252–263.
The authors address the problem of exact histogram specification and propose a method that is consistent with the human visual system. They also propose two watermarking techniques: the first one assigns a particular histogram as a water-

mark and the second uses the fact that the histogram specification transform is not exact.

[35] **'A Geometrical and Frequential Watermarking Scheme Using Similarities'**
P. Bas, J.-M. Chassery, F. Davoine, in Wong, Delp [10], pp. 264–272.
The authors argue that most of the existing watermarking schemes only map a mark on an image without geometric reference and therefore are not robust to geometric transformation. They present a scheme based on the modification of a collage map issued from a code used in fractal compression and add the watermark by introducing similarities in the image. Results show that the system is robust to translation rotation or cropping. The system is based on the Stephen-Harris detector.

[36] **'Digital Image Watermarking by Salient Point Modification – Pratical Results'**
P. M. J. Rongen, M. J. B. Maes, C. W. A. M. van Overveld, in Wong, Delp [10], pp. 273–282.
A new watermarking method that biases the geometric locations of salient points – that is points which are extrema for a given saliency function – in an image is presented. The watermark is a pseudo random subset of the pixel and the image is said to be watermark if a statistically significantly high percentage of the salient points lies on the watermark pattern. Detailed robustness test again filtering and JPEG compression are presented.

[37] **'Watermarking with quadratic residues'**
M. J. Atallah, S. S. Wagstaff, in Wong, Delp [10], pp. 283–288.
The authors suggest a way to modify any existing watermarking algorithm to improve its cryptographic robustness. The modification makes the algorithm dependent on the Legendre symbol (modulo a secret prime) of the data items in which the watermark should be stored.

[38] **'A Buyer-Seller Watermarking Protocol Based on Amplitude Modulation and the El Gamal Public Key Crypto System'**
N. Memon, P. W. Wong, in Wong, Delp [10], pp. 289–294.
The authors propose a watermarking protocol in which the buyer cannot fooled by the seller as it is the case for most existing systems.

[39] **'Blind digital watermarking for cartoon and map images'**
P.-C. Su, C.-C. J. Kuo, H.-J. M. Wang, in Wong, Delp [10], pp. 296–306.
The authors propose a wavelet-based, threshold adaptive watermarking scheme. It is an energy based frequency watermarking scheme that does not explicitly make use of the human visual system model. The watermark is added to some selected wavelet coefficients into selected subbands. The original is not required to extract the mark and the system is robust to JPEG compression.
`<http://biron.usc.edu/˜houngjyh/paper/ei99.eps>`.

[40] **'Watermarking of dither halftoned images'**
Z. Baharav, D. Shaked, in Wong, Delp [10], pp. 307–316.
The authors propose a method to watermark dither halftoned images by using a sequence of two optimal dither matrices. The also analyse a statistical model of the input to devise an optimal extraction algorithm.

[41] **'Marking and Detection of Text Documents Using Transform domain Techniques'**
Y. Liu, J. Mant, E. Wong, S. Low, in Wong, Delp [10], pp. 317–328.
The authors show that D.C.T.-based information hiding techniques are not suitable for text.

[42] **'Watermarking of 3D polygon based models with robustness against mesh simplification.'**
O. Benedens, in Wong, Delp [10], pp. 329–340.

This is an extended version of **1069**. Watermarks embedded in 3D models should be robust at least against mesh simplification. The author presents an alternative method that fills this requirement at the cost of a priori data needed for extraction. The embedding is done by moving the centre of mass of particular sets of vertices.

[43] **'Dither modulation: a new approach to digital watermarking and information embedding'**
B. Chen, G. W. Wornell, in Wong, Delp [10], pp. 342–353.
The authors argue that quantization index modulation systems offer significant performance advantages over previously proposed spread-spectrum and low-bit modulation systems in terms of trade-off between bit-rate and robustness to distortion.

[44] **'Algebraic Construction of a new Class of Quasi-Orthogonal Complex Arrays for Steganography'**
R. G. van Schyndel, A. Z. Tirkel, I. D. Svalbe, T. E. Hall, C. F. Osborne, in Wong, Delp [10], pp. 354–364.
The paper presents four methods of extending the dimensionality of 1D pseudo-random sequences and a new type of 2D array with good correlation properties that can be used to embed more than one watermark is described.

[45] **'Steganographic Image Transformation'**
S. Takano, K. Tanaka, T. Sugimura, in Wong, Delp [10], pp. 365–374.
This is a steganographic system based on fractional Brownian motion.

[46] **'R/D Optimal Data Hiding'**
P. Prandoni, M. Vetterli, in Wong, Delp [10], pp. 375–385.
The authors use a rate / distortion framework to maximise the amount of information one can hide into audio. A net throughput of 30 kbits / sec on 16-bit, 44.1 KHz PCM stereo signals is achieved.
`<http://lcavwww.epfl.ch/~prandoni/documents/SPIE.ps>`.

[47] **'A Technique for Image Data Hiding and Reconstruction without Host Image'**
J. J. Chae, B. S. Manjunath, in Wong, Delp [10], pp. 386–396.
This is a scheme to embed image into images based on multidimensional lattice codes that are inserted into the D.C.T. coefficients of the host image.

[48] **'Reversible Digital Images'**
K. T. Knox, in Wong, Delp [10], pp. 397–401.
This is an improved version of (Kurak et al. **1012**). Two simultaneous error diffusion calculations are run to ensure that both images have the same visual appearance as the original.

[49] **'A Secure Multicast Protocol with Copyright Protection'**
H. hua Chu, L. Qiao, K. Nahrstedt, in Wong, Delp [10], pp. 460–471.
The authors present a protocol for secure distribution of multicast data to a dynamic group. Encryption keys are re-issued on a periodical basis to all members of the group. Simultaneous use of watermarking and different encryption keys allow tracing illegal copies.

[50] **'An Architecture of Security Management Unit for Safe Host Multiple Agents'**
T. Gilmont, J.-D. Legat, J.-J. Quisquater, in Wong, Delp [10], pp. 472–483.
The authors propose a processor architecture allowing cipher code execution and cipher data processing using a non volatile memory to store secret keys and critical data. This allows features such as intellectual protection or itinerant agent hosting.

[51] **'Securing the Anonymity of Content Providers in the World Wide Web'**
T. Demuth, A. Rieke, in Wong, Delp [10], pp. 494–502.
The authors present the JANUS system used for server anonymisation.

[52] **'Watermarking by D.C.T. Coefficient Removal: A Statistical Approach to Optimal Parameter Settings'**
G. C. Langelaar, R. L. Lagendijk, J. Biemond, in Wong, Delp [10], pp. 2–13.
The authors enhance their earlier work ([8]) by using a statistical model of the D.C.T. coefficients and the embedding method to find a trade-off between the robustness of the watermark to JPEG compression, the number of D.C.T. blocks used for embedding, and the D.C.T. coefficient that can be discarded. Robustness to JPEG compression only is studied.
`<http://www-it.et.tudelft.nl/~gerhard/spie99.zip>`.

[53] **'Anonymous web transactions with Crowds'**
M. K. Reiter, A. D. Rubin, Communications of the ACM (USA), vol. 42 no. 2 pp. 32–38, Feb. 1999 , .
The authors describe how the Crowds system works – essentially, a group of users act as web forwarders for each other in a way that appears random to outsiders. They analyse the anonymity properties of the system and compare it with other systems. Crowds enables the retrieval of information over the web with only a small amount of private information leakage to other parties.

[54] **'Onion routing for anonymous and private Internet connections'**
D. Goldschlag, M. Reed, P. Syverson, Communications of the ACM (USA), vol. 42 no. 2 pp. 39–41, Feb. 1999 , .
The authors describe Onion routing mechanism and its application for privacy use.

[55] **'Consistent, yet anonymous, web access with LPWA'**
E. Gabber, P. B. Gibbons, D. M. Kristol, Y. Matias, A. Mayer, Communications of the ACM (USA), vol. 42 no. 2 pp. 42–47, Feb. 1999 , .
The authors describe the Lucent Personalised Web Assistant (LPWA), a system designed to provide aliases for web users. Each alias contains alias username, alias password, and alias email address. The privacy aspect of this system is discussed.

[56] **'Fingerprint feature extraction using Gabor filters'**
C. J. Lee, S. D. Wang, Electronics Letters of the IEE (UK), vol. 35 no. 4 pp. 288–290, 18 Feb. 1999 , .
The authors suggest using Gabor filter-based features directly extracted from grey-level fingerprint images as the input vectors to classifiers in their test database. The experiment shows 97.2% accuracy with 3-NN classifiers.

[57] **'Wavelet based watermarking method for digital images using the human visual system'**
Y. S. Kim, O. H. Kwon, R. H. Park, Electronics Letters of the IEE (UK), vol. 35 no. 6 pp. 466–468, 18 Mar. 1999 , .
A three-level watermarking based on the discrete wavelet transform (DWT) is suggested by the authors. Different weighing in the DWT is proposed, proportional to the energy in each band. The robustness of the method is examined, with the original image being necessary for watermark detection.

[58] **'Hidden Digital Watermarks in Images'**
C. T. Hsu, J. L. Taiwan, IEEE Transactions on Image Processing (USA), vol. 8 no. 1 pp. 58–68, Jan. 1999 , .
The authors present a discrete cosine transform-based algorithm for JPEG image watermarking and discuss the experimental results. The technique can survive image cropping, enhancement and JPEG lossy compression.

[59] **'A Digital Watermark Technique Based on the Wavelet Transform and Its Robustness on Image Compression and Transformation'**
H. Inoue, T. Katsura, A. Miyazaki, A. Yamamoto, IEICE Transactions on Fundamentals of Electronics, vol. E82-A no. 1 pp. 2–10, Jan. 1999 , .
The authors propose two digital watermarking schemes, both with the wavelet

coefficients built on a data structure called a zerotree (defined by Shapiro in IEEE Transactions Signal Processing 41.12). In one method, insignificant image coefficients are used for embedding the mark, while the other does it by modifying significant coefficients at coarse scales in perceptually important spectral components.

[60] **'Information hiding – a survey'**
F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, Proceedings of the IEEE (USA), vol. 87 no. 7 pp. 1062–1078, July 1999 , .
The authors provide an overview of information hiding, including steganography, digital watermarking and fingerprinting. They start off by clarifying the terminology, then describe a wide range of techniques that have been used in applications both ancient and modern. Finally they describe a number of attacks against these techniques and formulate general principles and theory.

[61] **'Multimedia watermarking techniques'**
F. Hartung, M. Kutter, Proceedings of the IEEE (USA), vol. 87 no. 7 pp. 1079–1107, July 1999 , .
The authors explain the common design requirements applied in all digital watermarking techniques. The state-of-the-art for digital watermarking is then exposed in great detail. Finally some existing attacks are listed and future possible trends explored.

[62] **'Perceptual watermarks for digital images and video'**
R. Wolfgang, C. I. Podilchuk, E. Delp, Proceedings of the IEEE (USA), vol. 87 no. 7 pp. 1108–1126, July 1999 , .
The authors present watermarking as a compromise between imperceptibility and robustness. An overview of visual models developed for image processing applications is presented. Two classes of perceptual watermarks are described: image-independent perceptual watermark and image-adaptive watermarks.

[63] **'Watermarking as communications with side information'**
I. J. Cox, M. L. Miller, A. L. McKellips, Proceedings of the IEEE (USA), vol. 87 no. 7 pp. 1127–1141, July 1999 , .
The authors examine the similarities and differences between digital watermarking and spread-spectrum communications and suggest that watermarking resembles Shannon's communication with side information at the transmitter and/or decoder.

[64] **'Statistical analysis of watermarking schemes for copyright protection of images'**
J. R. Hernández, F. Prez-Conzález, Proceedings of the IEEE (USA), vol. 87 no. 7 pp. 1142–1166, July 1999 , .
The authors use an statistical approach to study spread-spectrum based digital watermarking: a statistical formulation of the detection problem is given when the statistics of the original image are known and when they are unknown. Finally the authors apply these theoretical results to two practical examples.

[65] **'Digital watermarking for telltale tamper proofing and authentication'**
D. Kundur, D. Hatzinakos, Proceedings of the IEEE (USA), vol. 87 no. 7 pp. 1167–1180, July 1999 , .
The authors propose a system to detect image tampering using fragile watermarking. The method embeds the watermark by quantising the wavelet coefficients of the original image. This provides detection and localisation of modified areas of the image. The technique also tells which frequencies of the image have been modified.

[66] **'Copyright protection for electronic distribution of text documents'**
J. T. Brassil, S. Low, N. F. Maxemchuk, Proceedings of the IEEE (USA), vol. 87 no.

7 pp. 1181–1196, July 1999 , .
The authors provide an in-depth study of marking text documents (treated as images) and later decoding the marks after the documents has suffered various common distortions including photocopying. The authors also present different document distribution models and detail their initial publishing experiment with the IEEE journal on selected areas in communications.

[67] **'The use of watermarks in the protection of digital multimedia products'**
G. Voyatzis, I. Pitas, Proceedings of the IEEE (USA), vol. 87 no. 7 pp. 1197–1207, July 1999 , .
The authors give a general framework for modeling watermarking procedures including some general definitions and requirements.

[68] **'Towards unique identifiers'**
N. Paskin, Proceedings of the IEEE (USA), vol. 87 no. 7 pp. 1108–1227, July 1999 , .
The author discusses the creation and use of unique identifiers for intellectual property. Requirements, capacity issues and business issues are explored. Brief examples of existing identifiers (including some failures) are given.

[69] **'A perspective: the role of identifiers in managing and protecting intellectual property in the digital age'**
K. Hill, Proceedings of the IEEE (USA), vol. 87 no. 7 pp. 1228–1238, July 1999 , .
The author presents international object numbering requirements and their implementation in the Imprimatur and the MPEG-4 standard developments.

[70] **'Persistent access control to prevent piracy of digital information'**
P. Schneck, Proceedings of the IEEE (USA), vol. 87 no. 7 pp. 1239–1250, July 1999 , .
The author introduces a license management framework that aims at ensuring persistent protection of files. Some of the underlying techniques as well as examples and applications are also presented. Each protected file is encrypted and a license is associated to it.

[71] **'Secure delivery of images oven open networks'**
D. Augot, J.-M. Boucqueau, J.-F. Delaigle, C. Fontaine, E. Goray, Proceedings of the IEEE (USA), , 1999 , .
The authors show how digital watermarking can be integrated in public-key based security infrastructures. The Aquarelle (access control and intellectual property protection of distributed databases) and Octalis (secure broadcast networks) projects are given as example of such architectures.

[72] **'Copy protection for DVD video'**
J. A. Bloom, I. J. Cox, T. Kalker, J.-P. M. G. Linnartz, M. L. Miller, C. B. S. Traw, Proceedings of the IEEE (USA), vol. 87 no. 7, July 1999 , .
The authors give the latest development for the coming Digital Versatile Disk for video and in particular how digital watermarking is used to improve the security of the already fielded solutions.

[73] **'Fingerprint Classification by Directional Image Partitioning'**
R. Cappelli, A. Lumimi, D. Maio, D. Maltoni, IEEE Transactions on Pattern Analysis and Machine Intelligence (USA), vol. 21 no. 5 pp. 402–421, May 1999 , .
A new fingerprint classification method is suggested that uses dynamic masks for directional image partitioning. The authors argue for this approach being translation and rotation invariant and base the approach on grouping similar elements into more-or-less coherent regions that are in turn used for classification.

[74] **'On the general classification of nonlinear filters of m-sequences'**
L. J. Garcia-Villalba, A. Fuster-Sabatier, Information Processing Letters (Netherlands), vol. 5 pp. 227–232, 69 , .
The paper present a classification of nonlinear filtering pseudo-noise sequences (m-sequences) used in stream ciphers. It is based on the sequentialdecomposition

in cosets (a kth order nonlinear filter is identified with the sum of sequences associated with every cyclotomic coset of weight $leqk$). This kind of representation gives more information on the structural properties of such filters (possible periods, possible values of their linear complexity, number of different sequences, etc.).

[75] **'Algorithm hides data inside unaltered images'**
Anonymous, Information Security Monitor, vol. 14 no. 8 pp. 10, July 1999 , .
The article reports a newly patented steganographic method that hides information into the least significant bits of images and sound files.

[76] **'Improvement to a Method of Embedding Robust Watermarks into Digital Color Images'**
A. Shiozaki, IEICE Transactions on Fundamentals of Electronics, vol. E82-A no. 5 pp. 861–864, May 1999 , .
This letter suggests a modification of the author's watermarking method presented in the same journal (vE81-A, no10, 1998) so that the watermark can be extracted even without the original image.

[77] **'Multiresolution watermarking for images and video'**
W. Zhu, Z. Xiong, Y. Q. Zhang, IEEE Transactions on Circuits and Systems for Video Technology, vol. 9 no. 4 pp. 545–550, June 1999 , .
The authors present a watermarking technique using two- and three-dimensional discrete wavelet transforms.

[78] **'The mathematics of information coding, extraction, and distribution'**
G. Cybenko, D. P. O'Leary, J. Rissanen, Eds., vol. 107 of The IMA volumes in mathematics and its applications, Springer-Verlag, New York, U.S.A., 1999. ISBN 0-387-98665-0, Based on the proceedings of a workshop held in November 1996 at the Institute for Mathematics and its Applications.

[79] **'Copyright? Protection?'**
C. Dwork, in Cybenko et al. [78], pp. 31–47, ISBN 0-387-98665-0, Based on the proceedings of a workshop held in November 1996 at the Institute for Mathematics and its Applications.
The paper summarises three watermarking techniques (the first Digimarc's patent), J Brassil et al. (IEEE Infocom 94 pp. 1278-1287) and IJ Cox et al. (Info Hiding 96 pp. 185-206). The tracing traitors problem is then introduced by explaining the work of Fiat (Crypto 94 pp 257-270) and of Boneh and Shaw (Crypto 95 pp 452-465). The auther then exposes the advantages of her scheme (STOC 96 pp 489-498) that fights the problem by making sure that a huge amount of data has to be copied for proper description.

[80] **'International Conference on Acoustics, Speech and Signal Processing'**
IEEE Signal Processing Society, Phoenix, Arizona, USA, 15–19 Mar. 1999. ISBN 1-876346-19-1.

2 General background

[81] **'Information hiding: first international workshop'**
R. J. Anderson, Ed., vol. 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, May 1996. Springer-Verlag, Berlin, Germany. ISBN 3-540-61996-8.
This workshop on information hiding formed part of a six month research programme which was held in 1996 at the Isaac Newton Institute on Computer Security, Cryptography and Coding Theory.

<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[82] **'The Codebreakers – The Story of Secret Writing'**
D. Kahn, Scribner, New York, New York, U.S.A., 1996. ISBN 0-684-83130-9.
The classic work on the history of crypto also contains a fair bit of material on stego. This includes a classical Chinese practice of embedding the code ideogram at a prearranged place in a dispatch; the warning the Greeks received of Xerxes' intentions via writing underneath the wax of a writing tablet; various open and jargon codes; the trick of dotting successive letters in a covertext with secret ink, due to Aeneas the Tactician; Bacon's system of encoding using two slightly different typefaces; Madame Defarge's knitting, which contained the names of enemies of the French Republic; the Cardano grill, which picks out a subset of the words on a page as being significant; and of course the whole technology of secret inks, microdots and the rest. The word 'steganography' was coined in 1499 by Trithemius, who encoded letters as religious words in such a way as to turn covert messages into apparently meaningful prayers. People interested in policy aspects will be interested to read of the restrictions imposed by the USA in world war 2 to try and plug up as many channels as possible. The post banned a large class of objects, including chess games, crosswords, and newspaper clippings; lovers' X's were deleted; watch hands were shifted; orders for flowers could not specify either the kind of flower or the date of delivery; and items such as loose stamps and blank paper were replaced. Thousands of people were involved in reading mail, looking for language which appeared to be forced. They also rephrased telegrams; in one case, a censor changed 'father is dead' to 'father is deceased', which elicited the reply 'is father dead or deceased?'.

[83] **053340**, **'Cryptology in the 15th and 16th century'**
T. Leary, Cryptologia, vol. XX no. 3 pp. 223–242, July 1996 , .
This article discusses a number of cryptographic and steganographic systems used in the fifteenth and sixteenth centuries. Authors of books such as histories often concealed their names in case their work offended powerful factions; while a treatise on the subject was written by Bishop John Wilkins, later the Master of Trinity. He devised a number of schemes ranging from coding messages in music and string knots to invisible inks, described the principles of cryptanalysis by letter frequencies, and argued against those who opposed publication in the field: "it will not follow that everything must be suppressed which may be abused".

[84] **054101**, **'Stretching the Limits of Stegranography'**
R. J. Anderson, (Preproceedings).
The author provides a brief overview of the state of the art in steganography, and shows how public key steganography is possible — at least in the presence of a passive warden. The basic idea is that if the communicating parties can manipulate at least one out of n bits in the covertext, then the warden cannot distinguish the parity of successive blocks of n bits from random noise; accordingly these parity bits can be used to hide ciphertext in plain sight. Information theoretic limits of general steganography are also discussed, and it is shown that parity techniques can make many systems more efficient. Finally, the differential effectiveness of active and passive wardens is discussed.

[85] **054141**, **'The History of Steganography'**
D. Kahn, in Anderson [402], pp. 1–5.
The author describes the history of steganography from its origins in ancient times with letter marking and other techniques, through the development of invisible inks and microdots, and spread spectrum communications. In addition to these technological message concealment techniques, he discusses linguistic techniques, which he classifies into semagrams (which use sign language of some kind) and

open codes (in which certain key words have prearranged hidden meanings).
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[86] **054161**, **'The history of subliminal channels'**
G. J. Simmons, in Anderson [402], pp. 237–256.
The author tells the story of how subliminal channels were discovered in 1978. A system was designed to enable the Russians to check that only a certain percentage of minuteman silos were occupied, without letting them know which ones. This involved sensors in the silos that authenticated their signals by concatenated encryption: first a Russian algorithm would be used, then an American one. Simmons pointed out that if the Russians chose Rabin encryption, in which each plaintext can give rise to two possible ciphertexts, then a bit of unauthorised information could be leaked; ten such bits could locate a silo and thus enable the Russians to identify which silos were full. The choice of ElGamal signatures would have had a similar effect. He also recalls that the first military implementation of RSA — for controlling access to plutonium — used a modulus of only 334 bits.
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[87] **054156**, **'Information Hiding Terminology'**
B. Pfitzmann, in Anderson [402], pp. 347–350, Results of an informal plenary meeting and additional proposals.
The author reports terminology agreed at the plenary session of the first international workshop on information hiding, whose aim is to help workers in copyright marking, steganography, covert channels and related fields to avoid confusion and ambiguity. An embedded datatype (text, image etc) is hidden in a cover datatype, under the control of a key, giving a stego datatype. The recipient can then use the key (or a related one) to extract the embedded data.
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[88] **'Disappearing Cryptography – Being and Nothing on the Net'**
P. Wayner, AP Professional, Chestnut Hill, MA, 1996. ISBN 0-12-738671-8.
This books decribes many different techniques that people can use to hide information. This include error correction codes, compression algorithms, mimicry of texts (using statistical properties of natural languages or using ellaborated grammars), hiding in images or sound by modifying the least significant bits and spreading the message in the cover text. Secrecy of the meta-content of messages is also reviewed; this include for instance anonymous remailsers. For each technique both very simple and quite detailed (code is sometimes appended) explanations are given. This can be a good introduction to steganography for neofits as well as experts who might discover new interesting tricks.
<http://www.apnet.com/>.

[89] **'Optical document security'**
R. van Renesse, Artech House, 1997. ISBN 0-89006-982-4.
The rapidly growing interest in methods of hiding copyright marks in digital audio and video might prompt a thoughful person to ask about the techniques used by more traditional users of information hiding techniques, namely the companies that print documents such as passports and banknotes. Meanwhile, these companies have adopted all manner of tricks ranging from effects of physics and materials science, such as kinegrams, optically variable inks and partially metallised films, to alias band effects and other tricks which have direct analogues in the world of digital information hiding. The publication of this book on document security could scarcely be more timely. It provides fairly complete explanations of many of the effects used by modern security printers, together with a number

of samples and a reference CD. The explanation is pitched at the level of scientific explanation rather than training for forgery, but this is ideal for its legitimate purposes. This book should be read by everyone involved in intellectual property protection.

[90] **072102**, **'On The Limits of Steganography'**
R. J. Anderson, F. A. P. Petitcolas, IEEE Journal of Selected Areas in Communications, vol. 16 no. 4 pp. 474–481, May 1998, Special issue on copyright & privacy protection.
This journal version of [84] clarifies what steganography is and what it can do. It also outlines a number of approaches — many of them developed to hide encrypted copyright marks or serial numbers in digital audio or video — and presents a number of attacks on them. This leads to a discussion of the formidable obstacles that lie in the way of a general theory of information hiding systems. Finally, they show that public key information hiding systems exist, and are not necessarily constrained to the case where the warden is passive.
`<http://www.cl.cam.ac.uk/users/fapp2/papers/jsac98-limsteg/>`.

[91] **073142**, **'Digital Watermarking: Historical Roots'**
M. Kobayashi Tech. Rep. RT0199, I.B.M. Research, Tokyo Research Laboratories, Japan, Apr. 1997.
The author summarises briefly the history of steganography including Homer's report of Bellerophoron's trip to Lycia and Herodotus' story about the messenger's head which was shaved and tattooed. Then a brief account is given of recent research on text (**034110**, **054111**) and audio marking, followed by a summary of visible watermarking techniques for digital images as well as invisible techniques including **054106**, **054118**, **063131**.

[92] **073181**, **'Digital watermarking: an overview'**
G. Voyatzis, N. Nikolaidis, I. Pitas, in 9th European Signal Processing Conference (EUSIPCO'98), Island of Rhodes, Greece, 8–11 Sept. 1998, pp. 9–12. ISBN 960-7620-05-4.
The authors summarise the main features of watermarking schemes for still images, review the minimum steps involved in the implementation of their algorithm and discuss very briefly the robustness issues.

[93] **'Multimedia Data-Embedding and Watermarking Technologies'**
M. D. Swanson, M. Kobayashi, A. H. Tewfik, Proceedings of the IEEE, vol. 86 no. 6 pp. 1064–1087, June 1998 , .
The authors review in detail several algorithm for data hiding and digital watermarking into still images, audio and video. The article stresses the importance of the masking properties of the human perceptual systems to improve the robustness of marking systems and gives a brief summary of the history of the field.

[94] **'Information Hiding: Second International Workshop'**
D. Aucsmith, Ed., vol. 1525 of Lecture Notes in Computer Science, Portland, Oregon, U.S.A., 1998. Springer-Verlag, Berlin, Germany. ISBN 3-540-65386-4.

3 Subliminal channels

[95] **'Workshop on Communications Security (CRYPTO'83)'**
D. Chaum, Ed., Santa Barbara, California, U.S.A., 1984. IEEE, Plenum Press.

[96] **'The Prisoners' Problem and the Subliminal Channel'**
G. J. Simmons, in Chaum [95], pp. 51–67.
In order to get round the US government's prohibition on publishing work on steganography, Simmons introduced the following abstract model: Alice and Bob

are prisoners, and wish to hatch an escape plan. All their communications pass through the warden, Willy. If Willy sees any ciphertext in their messages, he will frustrate them by putting them into solitary confinement. Simmons shows that a message authentication without secrecy channel providing r bits of message authentication can be perverted to allow an $l < r$ bit covert channel between the transmitter and a designated receiver at the expense of reducing the message authentication capability to $r-l$ bits. Under quite reasonable conditions, the detection of even the existence of this covert channel can be made as difficult as the underlying cryptoalgorithm. In view of this open — but indetectable — existence, the covert channel was called the "subliminal" channel.

[97] **'Protocols for Data Security'**
R. DeMillo, M. Merritt, IEEE Computer, vol. 16 no. 2 pp. 39–50, Feb. 1983 , .
In one of the earliest papers on cryptographic protocol failure, the authors pointed out that a protocol for playing poker over the telephone leaked information via quadratic characters.

[98] **'The Subliminal Channel and Digital Signatures'**
G. J. Simmons, in Advances in Cryptology—EUROCRYPT '84. 1984, vol. 209 of Lecture Notes in Computer Science, Springer Verlag.
The author shows how subliminal channels can be implemented in the ElGamal and Schnorr signature schemes.

[99] **'Contemporary Cryptology – The Science of Information Integrity'**
G. J. Simmons, Ed., IEEE Press, New York, New York, U.S.A., 1992.

[100] **'How to Insure That Data Acquired to Verify Treaty Compliance Are Trustworthy'**
G. J. Simmons, In GJS88 [99], chapter 13, pp. 615–630.
This is one of a series of papers in which the author describes the evolution at Sandia National Laboratories of a solution to the problem of verifying compliance with a nuclear test ban treaty. Data from sensors placed on another country's territory must report certain types of information but not others.

[101] **021630**, **'Subliminal channels for signature transfer and their application to signature distribution schemes'**
K. Sakurai, T. Itoh, in Auscrypt 92, Gold Coast, Queensland, Australia, 13–16 Dec. 1992, Lecture Notes in Computer Science, Springer Verlag.
The parallel version of Fiat-Shamir has an extra subliminal channel. This can be used to implement distributed threshold verification. A distributed signature scheme is defined as one which requires the cooperation of all verifiers in order for the signature to be published.

[102] **022612**, **'The Subliminal Channels in the US Digital Signature Algorithm (DSA)'**
G. J. Simmons, in 3rd Symposium of State and Progress of Research in Cryptography, Rome, Italy, 15–16 Feb. 1993, pp. 35–54, Fondazione Ugo Bordoni.
The well known subliminal channel in El-Gamal is inefficient in that it allows only $\phi(p-1)$ different messages to be sent with the p session keys, but DSA allows the entire session key to be used, and thus q different messages can be sent to a recipient who shares the sender's secret key. Furthermore, DSA allows subliminal messages to be sent to a recipient who does not share this key, and thus (unlike El-Gamal) can combine signature and subliminal functions. This can be achieved, for example, by choosing r so that the quadratic character of (r mod p) mod q with respect to some prime lying between p and q encodes a bit.

[103] **023619**, **'Subliminal Communication is Easy Using the DSA'**
G. J. Simmons, in Eurocrypt 93, Lofthus, Norway, 23–27 May 1993, Lecture Notes

in Computer Science, pp. T65–T81, Page numbers given here are for preproceedings.
The author continues the discussion of subliminal channels in the digital signature algorithm. He focusses in this paper on the broadband channel – the one which requires the recipient to know the sender's secret key, and uses examples to compare it with the similar channel in the standard El-Gamal signature scheme. He concludes that DSA provides the best subliminal channels so far discovered.

[104] **031624**, **'Subliminal channels in the Digital Signature Algorithm'**
B. Schneier, Computer Security Journal, vol. 9 no. 2 pp. 57–63, 1993 , .
The Digital Signature Algorithm has several subliminal channels: these are covert communication channels that a signer can use to send a message to a specific receiver or observer. These channels are described and discussed in this article.

[105] **032631**, **'Subliminal Channels for Transferring Signatures: Yet Another Cryptographic Primitive'**
K. Sakurai, T. Itoh, IEICE Transactions on Fundamentals of Electronics, vol. E77-A no. 1 pp. 31–38, 1994 , .
This paper explores the transfer of signatures using the subliminal channels in the parallel version of the Fiat-Shamir identification scheme. It introduces a new notion, the 'privately recordable signature' which is generated by the interactive protocol between the signer and the verifier, and only the verifier can keep the signature (no third party can record it). In this scheme, the disclosure of the verifier's private coin turns the signature into an ordinary digital signature which can be verified with the signer's public key.

[106] **032633**, **'Subliminal Channels in the Digital Signature Algorithm'**
B. Schneier, PC Techniques, vol. 5 no. 2 pp. 72–76, June 1994 , .
The Digital Signature Algorithm has several subliminal channels, covert communication channels that a signer can use to send a message to a specific receiver. These subliminal channels are described and discussed in this article.

[107] **034412**, **'Subliminal Channels: Past and Present'**
G. J. Simmons, European Transaction on Telecommunications, vol. 5 no. 4 pp. 459–473, July / Aug. 1994 , .
This paper describes a protocol proposed in 1978 to monitor compliance with the SALT II treaty, and how the author found a potentially disastrous flaw in it – a subliminal channel which would have allowed the USSR to discover which Minuteman silos contained missiles. This discovery led to his subsequent work on the topic of subliminal channels, some of which is described. In particular, channels in the ElGamal and DSS digital signature scheme are compared, and it is shown that the DSS provides the most hospitable setting for subliminal communications discovered to date.

[108] **054603**, **'The Newton Channel'**
R. J. Anderson, S. Vaudenay, B. Preneel, K. Nyberg, in Anderson [402], pp. 151–156.
The authors show that ElGamal signatures modulo a prime p can be decomposed into separate signatures in the subgroups of Z_p^*. The signing key may be findable using discrete log computation techniques, or deliberately shared with some third party, module some of the distinct prime power factors of $p-1$ but not others. This gives rise to broadcast and narrowcast subliminal channels respectively. The construction settles in the negative a conjecture of Simmons that all broadband subliminal channels involve compromising the signing key. It also shows that the US digital signature standard is designed to minimise the subliminal channel capacity, rather than maximise it as had previously been thought.
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[109] **054604**, **'A Progress Report on Subliminal-Free Channels'**
M. Burmester, Y. G. Desmedt, T. Itoh, K. Sakurai, H. Shizuya, M. Yung, in Anderson [402], pp. 157–168.
The authors discuss the definition of a subliminal channel and point out some problems. For example, a player can always balk and refuse to complete a protocol if its outcome is going to be unfavourable to him. They review a number of signature and zero-knowledge schemes for subliminal freeness and present a coin flipping protocol that they claim to be subliminal free – although running it twice in succession is not.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[110] **061457**, **'Subliminal Channels: Some Recent Developments'**
G. J. Simmons, in RSA Data Security Conference, San Francisco, California, 28–31 Jan. 1997, RSA DSI Inc.

[111] **062621**, **'A note on error-correcting codes for authentication and subliminal channels'**
C. N. Yang, C. S. Laih, Information Processing Letters (Netherlands), vol. 62 no. 3 pp. 141–142, 14 Apr. 1997 , .
The authors discuss a scheme of Safavi-Naini and Seberry for embedding a subliminal channel in the McEliece public key cryptosystem, and show a way of neatly partitioning the set of possible encodings so that decoding becomes straightforward.

[112] **064155**, **'Self-synchronised Message Randomisation Method for Subliminal Channels'**
K. Kobara, H. Imai, in Information and Communications Security – First International Conference, Beijing, China, 11–14 Nov. 1997, vol. 1334 of Lecture Notes in Computer Science, pp. 325–334. ISBN 3-540-63696-X.
The authors address the problem of making a subliminal message recognisable to the intended recipient while remaining indistinguishable from random to third parties.

[113] **072153**, **'The History of Subliminal Channels'**
G. J. Simmons, IEEE Journal of Selected Areas in Communications, vol. 16 no. 4 pp. 452–462, May 1998, Special issue on copyright & privacy protection.
This is a journal version of [86].

[114] **072441**, **'Results Concerning the Bandwidth of Subliminal Channels'**
G. J. Simmons, IEEE Journal of Selected Areas in Communications, vol. 16 no. 4 pp. 463–473, May 1998, Special issue on copyright & privacy protection.
This journal version of **061457** discusses whether a protocol can ever be free of subliminal channels in view of the fact that one participant can simply refuse to continue in the context of a game-theoretic analysis of the behaviour of the prisoner and the warden. This leads to a redefinition of a subliminal free channel as one whose information content is indistinguishable from the output of a random source to the subliminal receiver; this is asymptotically achievable for any channel whose capacity is bounded away from zero. It goes onto consider the implications of the Newton Channel (**061602**); this leads to a refinement of the definition of broadband and narrowband channels.

[115] **'On Public-key Steganography in the Presence of an Active Warden'**
S. Craver Tech. Rep. RC20931, I.B.M. Research Division, T.J. Watson Research Center, Yorktown Heights, New York, U.S.A., July 1997.
It has been showed that public-key steganography was possible (**072102**) but the initial key exchange was still a problem. This difficulty leads the author to introduce the supraliminal channel, which is a very low bandwidth channel that an

attacker cannot afford to modify as it uses the most perceptually significant components of the cover object as a means of transmission. The supraliminal channel is blatant, robust and inconspicuous.

[116] **'Information hiding: first international workshop'**
R. J. Anderson, Ed., vol. 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, May 1996. Springer-Verlag, Berlin, Germany. ISBN 3-540-61996-8.
This workshop on information hiding formed part of a six month research programme which was held in 1996 at the Isaac Newton Institute on Computer Security, Cryptography and Coding Theory.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

4 Techniques for data hiding

4.1 Review papers

[117] **054106**, **'Techniques for data hiding'**
W. Bender, D. Gruhl, N. Morimoto, A. Lu, I.B.M. Systems Journal, vol. 35 no. 3 & 4 pp. 313–336, 1996 , .
The authors survey steganographic techniques used for hiding copyright marks, tamperproofing information and annotations in sound and images. The key is finding 'holes' in the signal that are not suitable for exploitation by compression algorithms, and to fill them with data in a way that remains invariant under a large class of signal transformations. They describe a number of algorithms, including Patchwork, which hides a bit of data in an image by increasing the differential luminance of a large number of pseudorandomly chosen pixel pairs, and echo hiding, which is also described in **054134** below.

[118] **061171**, **'Look, It's Not There – Digital watermarking is the best way to protect intellectual property from illicit copying'**
J. Zhao, BYTE, , Jan. 1997 , .
This general introduction to watermarking techniques discusses the general protection goals of this technology and the ideas underlying a number of implementations, particularly spread-sequence, frequency hopping and transform techniques.

[119] **'A review of watermarking and the importance of perceptual modeling'**
I. J. Cox, M. L. Miller, in Rogowitz, Pappas [121].
In a first section, the authors outline the desirable properties of watermarks. These properties depends on the intended use of the watermark: copyright control, authentication. Then, after emphasing the importance of perceptual modelling, and introducing a framework for watermarking they review several early papers (including **054118**, **054111**, **043140**, **054106**, **054163**).

[120] **'Exploring Steganography: Seeing the Unseen'**
N. F. Johnson, S. Jajodia, Computer, vol. 31 no. 2 pp. 26–34, Feb. 1998 , .
The authors review some recent steganographic tools freely available on the Internet. This includes: StegoDos, White Noise Storm and S-Tools. After a general introduction to steganography, the authors discuss advantages and weaknesses of each tools.

[121] **'Human Vision and Electronic Imaging II'**
B. E. Rogowitz, T. N. Pappas, Eds., vol. 3016, San Jose, California, U.S.A., Feb. 1997. The Society for Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIE), SPIE. ISBN 0-8194-2427-7, ISSN 0277-786X.

4.2 Information hiding into images

[122] **'Electronic Watermark'**
A. Z. Tirkel, G. A. Rankin, R. M. van Schyndel, W. J. Ho, N. R. A. Mee, C. F. Osborne, in Digital Image Computing, Technology and Applications (DICTA'93), Macquarie University, Sidney, 1993, pp. 666–673.
The authors suggest to use spread-spectrum technique to watermark still images.
`<http://www.physics.monash.edu.au/~ron/papers/DICTA93.html>`.

[123] **'A Digital Watermark'**
R. G. van Schyndel, A. Z. Tirkel, C. F. Osborne, in International Conference on Image Processing, Austin, Texas, U.S.A., 1994, IEEE, vol. 2, pp. 86–90.
The authors present two techniques to hide data into images. The first replaces the LSB of the image with an m-sequence while the second adds the m-sequence to the LSB of the image and uses auto-correlation to detect it later on.
`<http://www.physics.monash.edu.au/~ron/papers/AUSTIN.html>`.

[124] **'Assuring Ownership Rights for Digital Images'**
G. Caronni, in Reliable IT Systems (VIS'95), H. H. Brüggermann, W. Gerhardt-Häckl, Eds. 1995, pp. 251–263, Vieweg Publishing Company, Germany.
The author presents a procedure that embeds geometric patterns in digital images by modulating the brightness of chosen rectangles. Each user can be given a different pattern which enables the owner of the image to trace back illegal copies. The detection of the pattern requires the original image.
`<http://www.tik.ee.ethz.ch/~caronni/papers/givis-final.ps.gz>`.

[125] **'Towards Robust and Hidden Image Copyright Labeling'**
E. Koch, J. Zhao, in Workshop on Nonlinear Signal and Image Processing, Neos Marmaras, Greece, June 1995, IEEE, pp. 452–455.
The authors propose a method to embed a digital watermark in the D.C.T. domain of a picture. The image is divided into blocks (typically 8×8). The watermark is embedded by quantizing the D.C.T. coefficients and modifying some of them in such a way that a certain property (order in size) is verified.

[126] **'Embedding Robust Labels into Images for Copyright Protection'**
J. Zhao, E. Koch, in International Congress on Intellectual Property Rights for Specialised Information, Knowledge and New Technologies, Vienna, Austria, 21–25 Aug. 1995.
The authors describe two copyright marking schemes – one for embedding labels in JPEG compressed images, and one for black and white images. The former alters the quantisation table in the discrete cosine transform, and the latter encodes a bit according to whether a block of pixels is more black than white. Varying the table or block size allows the tradeoff between robustness and visibility to be selected.

[127] **'Image Authentication for a Slippery New Age'**
S. Walton, Dr. Dobb's journal of software tools, vol. 20 no. 4 pp. 18–26, Apr. 1995 , .
The article proposes a signature techniques for digital images (fragile watermark). A checksum is computed for the 7 most significant bit planes and then hidden in randomly chosen least significant bits.

[128] **'Copy Protection for Multimedia Data based on Labeling Techniques'**
G. C. Langelaar, J. C. A. van der Lubbe, J. Biemond, in 17th Symposium on Information Theory in the Benelux, Enschede, The Netherlands, May 1996.
The authors present a variant of Pitas' method [134] that divides the picture in small blocks and uses JPEG compression algorithm as feedback to choose a good random subset (see Pitas') for each block. The method is resistant to JPEG but not to simple transformation like rotation or cropping.
`<http://www-it.et.tudelft.nl/pda/smash/public/benlx96/benelux_cr.html>`.

[129] **054118**, **'A Secure, Robust Watermark for Multimedia'**
I. J. Cox, J. Kilian, T. Leighton, T. Shamoon, in Anderson [402], pp. 183–206.
The authors describe a technique for applying digital watermarks to both video and audio signals. The mark is inserted into the perceptually most significant spectral coefficients of the signal using ideas derived from spread spectrum communications. With marks inserted in still pictures using discrete cosine transform techniques, they show that marks can still be recovered after various common processing operations including scaling, jpeg compression, dithering and clipping. Even when the image is printed, xeroxed and scanned, a mark can still be recovered. A given image cannot be queried for ownership, however, as the original unwatermarked image is required as part of the extraction process.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[130] **061170**, **'A Digital Watermarking System for Multimedia Copyright Protection'**
J. Zhao, E. Koch, in Fourth ACM International Multimedia Conference, Boston, Massachussetts, 18–22 Nov. 1996, pp. 443–444, ACM. ISBN 0-89791-871-1.
The authors describe the main features of SysCoP, a digital watermarking system developed by the Fraunhofer Institute in Darmstadt. Label codes are embedded at locations determined with reference to extracted (geometric) features as well as a pseudorandom sequence generator.

[131] **'Transparent Robust Image Watermarking'**
M. D. Swanson, B. Zhu, A. H. Tewfik, in International Conference on Image Processing. IEEE, 1996, vol. III, pp. 211–214.
The authors propose a watermarking scheme for images that uses properties of the HVS. The watermark is a PN-sequence that is shaped using frequency masking. It is added in the D.C.T. domain. Spatial model is then used to verify that the watermark is invisible.
`<ftp://ftp.ee.umn.edu/pub/tewfik/1996/multimedia/wmk_icip96.ps.Z>`.

[132] **'Watermarking digital images for copyright protection'**
J. J. K. Ó Ruanaidh, W. J. Dowling, F. M. Boland, I.E.E. Proceedings on Vision, Signal and Image Processing, vol. 143 no. 4 pp. 250–256, Aug. 1996 , .
The authors present a private invisible watermarking technique for still images. The watermark is embedded in the D.C.T. domain by modulating the D.C.T. coefficients with a bi-directional coding. A technique to determine the number of bits to be placed at a given location is also presented. This leads to a more theoretical discussion on reliable transmission of watermarks.
`<http://cuiwww.unige.ch/~oruanaid/ieejnl.ps.gz>`.

[133] **'A Watermark for Digital Images'**
R. B. Wolfgang, E. J. Delp, in International Conference on Images Processing. IEEE, Sept. 1996, pp. 219–222, Lausanne, Switzerland.
The authors present a technique based on DSS. A PN-Sequence is added to the image. The two dimensional approach helps to detect where the image has been forged. The watermark survives JPEG compression to a certain extent.

[134] **063160**, **'A method for signature casting on digital images'**
I. Pitas, in International Conference on Image Processing, Sept. 1996, vol. 3, pp. 215–218.
The author present a watermarking method for images in the spatial domains: it modifies the LSB by increasing the contrast between to random subsets of pixels.

[135] **'Robust Data Hiding for Images'**
M. D. Swanson, B. Zu, A. H. Tewfik, in 7th Digital Signal Processing Workshop (DSP 96), Loen, Norway, Sept. 1996, IEEE, pp. 37–40.

The authors present two data hiding methods for images in D.C.T. domain. Both exploits the perceptual masking properties (spatial masking for the first one and frequency masking for the other) of the Human Visual System to strenghen the embedded watermark.
<ftp://ftp.ee.umn.edu/pub/tewfik/1996/multimedia/datahide.ps.Z>.

[136] **'A watermarking technique for digital imagery: further studies'**
R. B. Wolfgang, E. J. Delp, in International Conference on Imaging, Systems, and Technology, Las Vegas, Nevada, U.S.A., 30 June–3 July 1997, IEEE, pp. 279–287.
The authors give more details about the watermarking technique presented in their previous paper [9]. They study how the watermark survives paletization and I.B.M. attack [253].

[137] **063129**, **'A Low Cost Perceptive Digital Picture Watermarking Method'**
F. Goffin, J.-F. Delaigle, C. D. Vleeschouwer, B. Macq, J.-J. Quisquater, in Sethin, Jain [271], pp. 264–277.
The authors present a watermarking technique for pictures that uses a maximum length sequence to embed a message line by line in the cover image. A masking model of the human visual system and an edge detector filter are used to enhance the invisibility and robustness of the watermark.

[138] **063129**, **'Robust Labeling Methods for Copy Protection of Images'**
G. C. Langelaar, J. C. A. van der Lubbe, R. L. Lagendijk, in Sethin, Jain [271], pp. 298–309.
The authors present a watermarking technique for pictures that uses a maximum length sequence to embed a message line by line in the cover image. A masking model of the human visual system and an edge detector filter are used to enhance the invisibility and robustness of the watermark.

[139] **071112**, **'Secure Spread Spectrum Watermarking for Multimedia'**
I. J. Cox, J. Kilian, T. Leighton, T. Shamoon, IEEE Transactions on Image Processing, vol. 6 no. 12 pp. 1673–1687, Dec. 1997 , .
The authors argue for watermarks to be independent and identically distributed Gaussian random vectors placed in the most significant components of the image spectrum. They should then resist most signal processing operations as well as multiple watermark or collusion attacks.

[140] **071107**, **'Copyright Labeling of Digitized Image Data'**
S. Burgett, E. Koch, J. Zhao, IEEE Communications Magazine, vol. 36 no. 3 pp. 94–100, Mar. 1998 , .
The authors outline a method for embedding frequency-hopped randomly sequenced pulse position modulated code into JPEG images. Experimental results on this watermark resistance to some image processing methods are described.

[141] **'A M.A.P. identification criterion for D.C.T.-based watermarking'**
M. Barni, F. Bartolini, V. Cappellini, A. Piva, F. Rigacci, in 9th European Signal Processing Conference (EUSIPCO'98), Island of Rhodes, Greece, 8–11 Sept. 1998, pp. 17–20. ISBN 960-7620-05-4.
The paper addresses the problem of the reliable identification of a watermark in absence of the original image and present a maximum a posteriori criterion for extracting watermarks embedded using Cox algorithm [129].

[142] **073108**, **'A D.C.T.-domain system for robust image watermarking'**
M. Barni, F. Bartolini, V. Cappellini, A. Piva, Signal Processing, vol. 66 no. 3 pp. 357–372, May 1998, European Association for Signal Processing (EURASIP).
A digital watermarking algorithm similar to Cox's method (**054118**) is presented. However, the mark is always inserted in the same set of DCT coefficients after the usual zig-zag ordering, instead of using the 1000 largest DCT coefficients as Cox does. To achieve perceptual invisibility, only middle frequencies are modified. The

method, which can be used to embedd multiple marks, survives JPEG compression, lowpass filtering, cropping and rescaling.

[143] **073109**, **'Self-similarity based image watermarking'**
P. Bas, J. M. Chassery, F. Davoine, in 9th European Signal Processing Conference (EUSIPCO'98), Island of Rhodes, Greece, 8–11 Sept. 1998, European Association for Signal Processing, pp. 2277–2280. ISBN 960-7620-05-4.
The authors propose a method based on fractal coding to hide information in digital images. The algorithm can be applied to both luminance and DCT domains, but does not survive geometric transformations.

[144] **073158**, **'Robust image watermarking in the spatial domain'**
N. Nikolaidis, I. Pitas, Signal Processing, vol. 66 no. 3 pp. 385–403, May 1998, European Association for Signal Processing (EURASIP).
The authors enhance the digital watermarking algorithm presented in **063160**. Robustness to JPEG compression is addressed by increasing the luminance of small blocks of pixels (typically $2x2$ or $4x4$) rather than pixels only, hence shifting the watermark into the low frequencies. Properties of the human visual system are taken into account in the same way as JPEG. Finally the paper addresses robustness to line or row removal, cropping and statistical attacks. The latter problem is solved by using image-dependent watermarks.

[145] **073162**, **'Rotation, scale and translation invariant spread spectrum digital image watermarking'**
J. J. K. Ó Ruanaidh, T. Pun, Signal Processing, vol. 66 no. 3 pp. 303–317, May 1998, European Association for Signal Processing (EURASIP).
The authors explain how integral transform-based invariants for images can be used to improve the robustness of digital watermarking systems. The watermark is embedded in a domain which is invariant to rotation and scaling by using the Fourier-Mellin transform, or equivalently, the Fourier transform on a log-polar map.
<http://www1.elsevier.nl/cas/tree/store/sigpro/sub/1998/66/3/1170.pdf>.

[146] **073176**, **'Image and watermark registration'**
A. Z. Tirkel, C. F. Osborne, T. E. Hall, Signal Processing, vol. 66 no. 3 pp. 373–383, May 1998, European Association for Signal Processing (EURASIP).
The authors show how to construct binary arrays suitable for embedding as watermarks on images. Perfect maps, perfect even and odd binary arrays, *m*-arrays and quasi-*m*-arrays are examined.

[147] **'Robust image watermarking in the subband or discrete cosine transform domain'**
D. Tzovaras, N. Karagiannis, M. G. Strintzis, in 9th European Signal Processing Conference (EUSIPCO'98), Island of Rhodes, Greece, 8–11 Sept. 1998, pp. 2285–2288. ISBN 960-7620-05-4.
An adaptive extension of Pitas' method [134] is used to embed a watermark in the lowpass image using the D.C.T. or the Haar Transform.

[148] **073183**, **'A blind wavelet based digital signature for image authentication'**
L. Xie, G. R. Arce, in 9th European Signal Processing Conference (EUSIPCO'98), Island of Rhodes, Greece, 8–11Sept. 1998, pp. 21–24. ISBN 960-7620-05-4.
The authors propose a content based digital image signature system. The weak watermark is embedded in the LL component of the wavelet transform domain of he picture and is based on the edges of the images. The information capacity of the algorithm is determined.

[149] **073139**, **'Content Based Watermarking of Images'**
M. S. Kankanhalli, R. K. R. Ramakrishnan, [404], pp. 61–70.

The authors present a spatial or D.C.T. based watermarking technique that uses a just noticeable distortion mask. This is similar to **072141**. The method also includes a content based classification to separate edges from smooth areas which are marked in a different way.

[150] **073141**, **'Generation of the signature with the structured information of the image'**
H. Kinoshita, M. Satoh, in 9th European Signal Processing Conference (EUSIPCO'98), Island of Rhodes, Greece, 8–11Sept. 1998, pp. 2273–2276. ISBN 960-7620-05-4.
The authors show how to generate an image signature based on picture structure information that remains invariant during some of the usual filtering operations. The information in question includes the picture's centre of gravity, size, its colours and the shape of textured regions.

[151] **073157**, **'Non-invertible statistical wavelet watermarking'**
G. Nicchiotti, E. Ottaviano, in 9th European Signal Processing Conference (EUSIPCO'98), Island of Rhodes, Greece, 8–11 Sept. 1998, pp. 2289–2292. ISBN 960-7620-05-4.
A watermark is embedded by applying Pitas' statistical method to the coefficients of the residual of the wavelet decomposition of a image.

[152] **074112**, **'A Virtual Image Cryptosystem Based upon Vector Quantization'**
M. S. H. T S Chen, C C Chang, IEEE Transaction on Image Processing, vol. 7 no. 10 pp. 1485–1488, Oct. 1998 , .
The authors present an encryption and steganographic technique for images. The secret image is compressed and the main parameters needed for reconstruction are enciphered using DES. The encrypted image is hidden in a cover image.

[153] **074115**, **'Watermarking algorithm based on a human visual model'**
J. F. Delaigle, C. De Vleeschouwer, B. Macq, Signal Processing, vol. 66 no. 3 pp. 319–335, May 1998, European Association for Signal Processing (EURASIP).
The authors detail a human visual model that is used later in a frequency hoping spread spectrum based watermarking algorithm for greyscale still images. A masking criterion derived from the HVM guaranties the invisibility of the watermark. Robustness against to AWGN, JPEG compression, low pass filtering and collision.
`<http://www1.elsevier.nl/cas/tree/store/sigpro/sub/1998/66/3/1171.pdf>`.

[154] **074140**, **'Digital watermarking using multiresolution wavelet decomposition'**
D. Kundur, D. Hatzinakos, in International Conference on Acoustic, Speech and Signal Processing (ICASP), Seattle, Washington, U.S.A., May 1998, IEEE, vol. 5, pp. 2969–2972.
A binary watermark is hidden in a chosen level discrete wavelet decomposition of an image by changing the relative position of the median of three coefficients taken from the horizontal, diagonal and vertical detail coefficients. The extraction does not require the original image but a copy of the embedded watermark, which is compared to the extracted one.

[155] **074144**, **'Generating Robust Digital Signature for Image/Video Authentication'**
C.-Y. Lin, S.-F. Chang, in Dittmann et al. [405], pp. 49–54.
The papers gives an example of 'robust' digital signatures for image authentication. This is a variant of Friedman's paper (**043125**). Rather than signing the full image, only a set of features (derived from the D.C.T. coefficient) is signed. So contrary to **043125** two images do not have to be bit/bit the same to give the same signature. The schemes allows users to localise where images have been edited, engineered, etc.

[156] **074160**, **'A Method for Watermark Casting on Digital Images'**
I. Pitas, IEEE Transactions on Circuits and Systems for Video Technology, vol. 8 no. 6 pp. 775–780, 1998 , .
This is a journal version of **063160**. The robustness of the watermarking system is evaluated with respect to AWGN and JPEG compression (up to 4:1).

[157] **074165**, **'Automatic visible watermarking of images'**
A. R. Rao, G. W. Braudaway, F. C. Mintzer, in van Renesse [403].
A linear regression model and image texture measurements are used to automate the adjustment of visible watermark intensity.

[158] **'Fast Public-Key Watermarking of Compressed Video'**
F. Hartung, B. Girod, in International Conference on Image Processing (ICIP'97), Santa Barbara, California, U.S.A., Oct. 1997, IEEE, vol. I, pp. 528–531. ISBN 0-8186-8183-7.
The authors a spread spectrum based public-key watermarking algorithm for video. Only one bit in n of the spread sequence is made public. This reduces the robustness of the watermark but allow public checking without enabling removal of the full watermark.
`<http://www-nt.e-technik.uni-erlangen.de/~hartung/publications/ icip97.ps.gz>`.

[159] **'A Method of Embedding Robust Watermarks into Digital Color Images'**
K. I. Hashida, A. Shiozaki, IEICE Transactions on Fundamentals of Electronics, vol. E81-A no. 10 pp. 2133–2137, Oct. 1998 , .
The authors present a new method for embedding watermarks into the spatial domain of a color image. It should be robust to withstand JPEG compression and brightness / contrast conversion. Also, the ID patterns can be extracted from different parts of an image.

[160] **'Image watermarking using block site selection and D.C.T. domain constraints'**
A. Bors, I. Pitas, Optics Express, vol. 3 no. 12 pp. 512–523, 7 Dec. 1998 , .
A watermark algorithm based on imposing constraints in the D.C.T. domain was proposed by the authors. Random image blocks are selected via a Gaussian network classifier and D.C.T. coefficients in these blocked are modified to satisfy some predefined constraints. The original image is not required for watermark detection and simulations showed this method is resistant to JPEG compression and filtering.
<http://epubs.osa.org/oearchive/source/7091.htm>.

[161] **'Wavelet-based digital image watermarking'**
H.-J. M. Wang, P.-C. Su, C.-C. J. Kuo, Optics Express, vol. 3 no. 12 pp. 491–496, 7 Dec. 1998 , .
The authors described a wavelet-based watermarking scheme, which does not require the original image for detection. The watermark is embedded in the significant coefficients in various sub-bands, except the lowest frequency one. The detection process is based on truncated wavelet coefficients. Experimental results show that this scheme is robust against distortion from common signal processing techniques.
<http://epubs.osa.org/oearchive/source/7081.htm>.

[162] **'Wavelet transform based watermark for digital images'**
X.-G. Xia, C. G. Boncelet, G. R. Arce, Optics Express, vol. 3 no. 12 pp. 497–511, 7 Dec. 1998 , .
A watermarking scheme in the wavelet domain was proposed. Watermark is embedded in the form of a random sequence in the large coefficients in middle frequency bands. The decoding process requires the original image and is based on

hierarchical correlation of coefficients at different sub-bands. The proposed scheme was shown to be robust against distortion caused be filtering or compression.
<http://epubs.osa.org/oearchive/source/7038.htm>.

[163] **'Reliable Blind Information Hiding for Images'**
L. M. Marvel, C. G. Boncelet, Jr., C. T. Retter, in Aucsmith [369], pp. 48–62.
Spread spectrum and error-control techniques are used to hide and recover messages into still images. The amount of additive random noise is controlled with Wiener filter based on the regional statistics of the image. The steganographic technique can embed up to 5kb into a 512×512 pixels image with a SNR around 32 dB.

[164] **'Information hiding: first international workshop'**
R. J. Anderson, Ed., vol. 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, May 1996. Springer-Verlag, Berlin, Germany. ISBN 3-540-61996-8.
This workshop on information hiding formed part of a six month research programme which was held in 1996 at the Isaac Newton Institute on Computer Security, Cryptography and Coding Theory.
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[165] **'Storage and Retrieval for Image and Video Database V'**
I. K. Sethin, R. C. Jain, Eds., vol. 3022, San Jose, California, U.S.A., Feb. 1997. The Society for Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIE), SPIE. ISBN 0-8194-2433-1, ISSN 0277-786X.

[166] **'6th ACM International Multimedia Conference (ACM Multimedia'98)'**
ACM, Bristol, England, Sept. 1998. ISBN 1-58113-036-8.

[167] **'Multimedia and Security – Workshop at ACM Multimedia'98'**
J. Dittmann, P. Wohlmacher, P. Horster, R. Steinmetz, Eds., vol. 41 of GMD Report, Bristol, United Kingdom, Sept. 1998. ACM, GMD – Forschungszentrum Informationstechnik GmbH, Darmstadt, Germany.

[168] **'Optical Security and Counterfeit Deterrence Techniques II'**
R. L. van Renesse, Ed., vol. 3314, San Jose, California, U.S.A., 28–30 Jan. 1998. The Society for Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIE), SPIE. ISBN 0-8194-2556-7, ISSN 0277-786X.

[169] **'Information Hiding: Second International Workshop'**
D. Aucsmith, Ed., vol. 1525 of Lecture Notes in Computer Science, Portland, Oregon, U.S.A., 1998. Springer-Verlag, Berlin, Germany. ISBN 3-540-65386-4.

4.3 Information hiding into text

[170] **034110**, **'Electronic Marking and Identification Techniques to Discourage Document Copying'**
J. Brassil, S. Low, N. Maxemchuk, L. O'Garman, in Infocom, Toronto, Canada, June 1994, IEEE, pp. 1278–1287.
The authors describe an AT & T system to discourage illegal document copying by marking documents with line-shift encoding. Successive lines of text are shifted up or down by $1/300''$, thereby encoding a serial number. Experiments on postscript documents showed that even third photocopies could be scanned and decoded with very few errors; different detection techniques are discussed, as are the effects of image defects and the countermeasures available to infringers.
<ftp://ftp.research.att.com/dist/brassil/infocom94.ps>.

[171] **034157**, **'Electronic Document Distribution'**
N. F. Naxemchuk, AT & T Technical, vol. 73 no. 5 pp. 73–80, Sept.–Oct. 1994 , .

This article describes techniques developed by Bell labs to make it easier to identify people who redistribute electronic documents. Identifying marks can be encoded in line spacing, word spacing and font features; their relative resistance to photocopying and to various erasure strategies is discussed. Such techniques can be used, for example, to embed a purchaser's name and credit card number in a document. A trial run is scheduled for an issue of the IEEE Journal on Selected Areas in Communications in 1995.

[172] **'Hiding Information in Documents Images'**
J. Brassil, S. Low, N. F. Maxemchuk, L. O'Gorman, in Conference on Information Sciences and Systems (CISS-95), Mar. 1995.
The authors present a marking technique for text document images that uses word shifting. Although the image of the original document is not required, a certain amount of information about it is mandatory.
`<ftp://ftp.research.att.com/dist/brassil/1995/ciss95.ps.Z>`.

[173] **'Document Marking and Identification using Both Line and Word Shifting'**
S. H. Low, N. F. Maxemchuk, J. T. Brassil, L. O'Gorman, in Infocom'95, Apr. 1995.
In previous experiments (see [170]), the authors noticed that there were two main distortion directions in paper documents depending of the orientation of the paper in the printer or photocopier. Using both word and line shifting makes the scheme more robust to distortions in both directions.
`<ftp://ftp.research.att.com/dist/brassil/1995/infocom95.ps>`.

[174] **054111**, **'Watermarking Document Images with Bounding Box Expansion'**
J. Brassil, L. O'Gorman, in Anderson [402], pp. 227–235.
The authors develop their work in [170], in which documents were marked by shifting lines, to shifting individual words. This has the effect of increasing the size of the box that bounds a particular piece of text by a few pixels, and turns out to be measurable even on a third generation photocopy.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[175] **064119**, **'Hiding the Hidden: A Software System for Concealing Ciphertext in Innocuous Text'**
M. Chapman, G. Davida, in Information and Communications Security — First International Conference, Beijing, China, 11–14 Nov. 1997, vol. 1334. ISBN 3-540-63696-X.
The authors give some examples of how ciphertext can be used to generate pseudo English text by passing it through various decompression routines. They give samples rendered in the style of Shakespeare, Federal Reserve English and Aesop's Fables.

[176] **071150**, **'Document Identification for Copyright Protection Using Centroid Detection'**
S. H. Low, N. F. Maxemchuk, A. P. Lapone, IEEE Transactions on Communication, vol. 46 no. 3 pp. 372–383, Mar. 1998 , .
The authors describe a text document watermarking method that shifts selected lines of text vertically, or moves words horizontally, on different copies of a document. A prototype implementation is presented together with experimental results that show a high degree of robustness against scanning, faxing and photocopying.

[177] **072132**, **'Performance Comparison of Two Text Marking Methods'**
S. H. Low, N. F. Maxemchuk, IEEE Journal on Special Areas in Communications, vol. 16 no. 4 pp. 561–572, May 1998 , .
Two maximum-likelihood detectors are proposed to detect marks in printed documents. The marking itself uses both line and word shifting. The detection either uses the original unwatermarked document to perform a correlation detection or does a centroid detection. The former seems to giver better results than the latter.

[178] **072141**, **'Image-Adaptive Watermarking Using Visual Models'**
C. I. Podilchuk, W. Zeng, IEEE Journal on Special Areas in Communications, vol. 16 no. 4 pp. 525–539, May 1998 , .
The authors use a DCT-based or wavelet-based framework for frequency decomposition of still images. They use this decomposition in a perceptual model which returns the amount of just noticeable difference that can be tolerated at every location and thus shows where a watermark should be placed.

[179] **'Information hiding: first international workshop'**
R. J. Anderson, Ed., vol. 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, May 1996. Springer-Verlag, Berlin, Germany. ISBN 3-540-61996-8.
This workshop on information hiding formed part of a six month research programme which was held in 1996 at the Isaac Newton Institute on Computer Security, Cryptography and Coding Theory.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

4.4 Information hiding into audio

[180] **054134**, **'Echo hiding'**
D. Gruhl, W. Bender, A. Lu, in Anderson [402], pp. 295–315.
The authors describe how to embed data in an audio signal at typically 16 bits per second by manipulating the echo characteristics of the signal below the level of perceptibility. This is achieved using cepstral transforms and is much more robust against lossy compression techniques than simple noise addition. It is also robust against D/A conversion, but is challenged by gaps of silence, such as inter-word pauses in speech. In addition to copyright protection, this can be used for applications such as annotation, captioning and the automatic monitoring of radio advertisements.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[181] **'Digital Watermarks for Audio Signals'**
L. Boney, A. H. Tewfik, K. N. Hamdy, in International Conference on Multimedia Computing and Systems, Hiroshima, Japan, 17–23 June 1996, IEEE, pp. 473–480.
This is a variant of the direct spread spectrum technique. In this scheme, the watermark is a PN-sequence shaped by a filter that approximates the frequency masking characteristics of the human auditory system. Thus the quality of the marked sound is improved, compare with a simple spread spectrum technique. However the energy given to the watermark, being localised in the frequency domain, is spread in the time domain and can introduce some pre-echo effects. So the filtered PN-sequence is weighted in the time domain.

[182] **'Digital Watermarks for Audio Signals'**
L. Boney, A. H. Tewfik, K. N. Hamdy, in European Signal Processing Conference (EUSIPCO'96), Trieste, Italy, Sept. 1996.
Same as [181].

[183] **064118**, **'Critical Analysis of Security in Voice Hiding Techniques'**
L. W. Chang, I. S. Moskowitz, in Information and Communications Security – First International Conference, Beijing, China, 11–14 Nov. 1997, vol. 1334 of Lecture Notes in Computer Science, pp. 203–216, Springer Verlag. ISBN 3-540-63696-X.
The authors consider four basic techniques for hiding data steganographically in a voice message: low-bit coding, phase coding, spread spectrum embedding and echo hiding. They analyse the available bandwidth and how this is affected if an opponent perturbs the signal by adding noise, bandpass filtering or resampling.

[184] **073110**, **'Robust audio watermarking in the time domain'**
P. Bassia, I. Pitas, in 9th European Signal Processing Conference (EUSIPCO'98), Island of Rhodes, Greece, 8–11 Sept. 1998, pp. 25–28. ISBN 960-7620-05-4.
The implementation employs a dual tree of wavelet filters to obtain the real and imaginary parts of the complex wavelet coefficients. This introduces limited redundancy and allows the transform to provide approximate shift invariance and directionally selective filters.

[185] **073173**, **'Robust audio watermarking using perceptual masking'**
M. D. Swanson, B. Zhu, A. H. Tewfik, L. Boney, Signal Processing, vol. 66 no. 3 pp. 337–355, May 1998, European Association for Signal Processing (EURASIP).
This is a variant of the direct spread spectrum technique. The watermark is a PN-sequence shaped using the psycho-acoustic model I of MPEG. It is added directly to the signal. Robustness to noise addition, compression and resampling is analysed in the paper. In order to solve the deadlock attack (**063115**) the authors apply the idea of dual watermarking presented in (**072157**).

[186] **074151**, **'Digital Watermarking and its Influence on Audio Quality'**
C. Neubauer, J. Herre, in 105th Convention of the Audio Engineering Society, San Francisco, California, U.S.A., 26–29 Sept. 1998.
The paper investigates the audio quality of a watermarking scheme presented at the second workshop on information hiding. It includes results of objective and subjective measurements.

[187] **074172**, **'Audio Watermarking and Data Embedding – Current State of the Art, Challenges and Future Directions'**
M. D. Swanson, B. Zhu, A. H. Tewfik, in Dittmann et al. [405].
The authors reviews in detailed the I.F.P.I. requirements and the challenges for embedding techniques in audio signals. They argue that double blind testing are not enough and one should be more concerned about the final output, that is what the end user will listen to. They also review the state-of-the art algorithms and argue that capacity is inversely proportional to robustness and also depends on the initial representation. Finally they acknowledge that time-scaling is one of the most challenging attack for audio marking.

[188] **'Intellectual property protection systems and digital watermarking'**
J. Lacy, S. R. Quackenbush, A. R. Reibman, J. H. Snyder, Optics Express, vol. 3 no. 12 pp. 478–484, 7 Dec. 1998 , .
The authors discuss music piracy, how the availability of various technologies (such as good compression) affects it, different system-level vulnerabilities of copyright marking mechanisms, and their likely future role. They argue that quantisation should be integrated with compression and present a method for MP3 which manipulates quantisation tables. They provide empirical results for an implementation with AAC.
`<http://epubs.osa.org/oearchive/source/7085.htm>`.

[189] **'Continuous Steganographic Data Transmission Using Uncompressed Audio'**
C. Neubauer, J. Herre, K. Brandenburg, in Aucsmith [369], pp. 208–217.
DSSS modulation is used to hide information into audio signals. Masking properties of the HAS are applied to weight the energy level of the watermark in a similar way as **073173**.

[190] **'Information hiding: first international workshop'**
R. J. Anderson, Ed., vol. 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, May 1996. Springer-Verlag, Berlin, Germany. ISBN 3-540-61996-8.
This workshop on information hiding formed part of a six month research programme which was held in 1996 at the Isaac Newton Institute on Computer

Security, Cryptography and Coding Theory.
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[191] **'Multimedia and Security – Workshop at ACM Multimedia'98'**
J. Dittmann, P. Wohlmacher, P. Horster, R. Steinmetz, Eds., vol. 41 of GMD Report, Bristol, United Kingdom, Sept. 1998. ACM, GMD – Forschungszentrum Informationstechnik GmbH, Darmstadt, Germany.

[192] **'Information Hiding: Second International Workshop'**
D. Aucsmith, Ed., vol. 1525 of Lecture Notes in Computer Science, Portland, Oregon, U.S.A., 1998. Springer-Verlag, Berlin, Germany. ISBN 3-540-65386-4.

4.5 Information hiding into video

[193] **043140**, **'Video-Steganography: How to Secretly Embed a Signature in a Picture'**
K. Matsui, K. Tanaka, Journal of the Interactive Multimedia Association Intellectual Property Project, vol. 1 no. 1 pp. 187–205, Jan. 1994 , .
The authors discuss schemes to embed copyright messages in pictures compressed using a number of different signal processing schemes, including predictive coding, ordered dithering, facsimile and discrete cosine transform. For example, fax messages are signed by replacing the rightmost pixel of each line with the next bit of the signature.

[194] **063131**, **'Watermarking of MPEG-2 encoded video without decoding and re-encoding'**
F. Hartung, B. Girod, in Freeman et al. [209], pp. 264–273.
The authors present a DSS based watermarking technique for MPEG-2 video streams. The input and the output are both MPEG-2. The information bits are first spread and then modulated using a PN sequence; the D.C.T. of this watermark is then added to the D.C.T. of the orignal MPEG stream. A drift compensation mechanism is used in the process.

[195] **064124**, **'Enabling technology for the trading of MPEG-encoded video'**
A. S. Jana Dittmann, in Information Security and Privacy: Second Australasian Conference, Sydney, Australia, 7–9 July 1997, vol. 1270 of Lecture Notes in Computer Science, pp. 314–324, Springer-Verlag. ISBN 3-540-63232-8.
The paper describes protocols to support copyright protection and support for 'Try and Buy' transactions in which the buyer receives video material of an inferior quality for evaluation, and when the payment is made can get the original quality. The idea is to apply encryption to the SNR scalable extension of MPEG coded images. The video stream is actually delivered in in two components: a lower grade used for the 'Try' phase and an encrypted enhancement layer which is delivered only after payment.

[196] **064125**, **'A Technical Approach to the Transparent Encryption of MPEG-2 Video'**
A. S. J Dittmann, in Third IFIP TC6/TC11 Working Conference on Communications and Multimedia Security, Athens, Greece, 22–23 Sept. 1997, pp. 215–226, Chapman and Hall. ISBN 0-412-81770-5.
This is another version of the work described in [195].

[197] **072157**, **'Multiresolution Scene-Based Video Watermarking Using Perceptual Models'**
A. H. T. M D Swanson, B Zhu, IEEE Journal on Special Areas in Communications, vol. 16 no. 4 pp. 540–550, May 1998 , .
The authors propose a watermarking system based on a perceptual model which

controls where in the image the strength of the watermark can be increased. The system is also scene based to allow extraction of the watermark from a reduced number of frames. Marks are added in the temporal wavelet transform domain of the video.

[198] **073121**, **'Robust MPEG Video Watermarking Technologies'**
J. Dittmann, M. Stabenau, R. Steinmetz, [404], pp. 71–80.
Two marking method for MPEG video are presented. The first is based on **043134** and the second on overlaying patterns with power concentrated in low frequencies. Both are enhanced with smooth-block / edge detection and strong error correction codes. Contrary to other systems, a watermark is embedded in each frame of the video on the ground that some people might be interested to copy a single image of a video.

[199] **073135**, **'Watermarking of uncompressed and compressed video'**
F. Hartung, B. Girod, Signal Processing, vol. 66 no. 3 pp. 283–301, May 1998, European Association for Signal Processing (EURASIP).
The authors present a direct sequence spread spectrum technique which can embed watermarks both into uncompressed and compressed video sequences. The first technique regards the video signal as a one-dimensional signal acquired by line scanning. The embedded signal is amplified to exploit the temporal and spatial phenomena of the HVS. The second technique generates a watermark signal per frame and adds it directly in the D.C.T. domain avoiding the need to uncompress completely the video stream. The performance of the system is illustrated with various BER tables.

[200] **073151**, **'MPEG PTY-Marks: Cheap Detection of Embedded Copyright Data in DVD-Video'**
J.-P. M. G. Linnartz, J. C. Talstra, in Quisquater et al. [251], pp. 221–240.
The authors present a marking system for MPEG video based on the asymmetry in complexity between encoding a frame as a particular picutre type (PTY) versus detecting that picture type. Within each group of pictures (GOP) P-frames denotes '0' and B-frames denotes '1'. Survey of existing material show that only certain patterns occur. Hence the authors propose a 'PTY-alphabet' constructed as a Hamming code detailed in the paper and containing different patterns. 64 bits of information are encoded in 10 seconds of video without deterioration of the image quality.

[201] **074119**, **'Robust MPEG Video Watermarking Technologies'**
J. Dittmann, M. Stabenau, R. Steinmetz, in Dittmann et al. [405], pp. 113–122.
This is another version of [198].

[202] **074129**, **'Digital Watermarking for Compressed Video'**
F. Hartung, J. K. Su, B. Girod, in Dittmann et al. [405], pp. 77–79.
This is an overview of [199].

[203] **074141**, **'Applying Encryption to Video Communication'**
T. Kunkelmann, in Dittmann et al. [405], pp. 41–47.
The author presents various partial encryption methods for video which have been proposed over the last few years: SEC-MPEG, encryption of the intracoded frames only, permutation of the D.C.T. blocks, etc. He expands these results to scalable video coding.

[204] **074150**, **'Non-Invertible Watermarking Methods for MPEG Video and Audio'**
K. Nahrstedt, L. Qiao, in Dittmann et al. [405], pp. 93–98.
The authors presents a watermarking system which survives the dead-lock attack (**063115**): the method which is proved to be non-invertible uses the DES of the number of non zero D.C.T. coefficient as watermark.

[205] **'Digital Watermarking: From Concepts to Real-Time Video Applications'**
C. Busch, W. Funk, S. Wolthusen, IEEE Computer Graphics and Applications, vol. 19 no. 1 pp. 25–35, Jan. / Feb. 1999 , .
The authors present an algorithm for watermarking and monitoring video streams in a TV-broadcasting environment. It is based on Koch's algorithm, but the D.C.T. has been improved for real-time applications and it adds checks of edges and textures to avoid artifacts in the watermarked video sequences. They do not take into account geometrical distortions.

[206] **'Steganography in a Video Conferencing System'**
A. Westfeld, G. Wolf, in Aucsmith [369], pp. 32–47.
The authors present a steganographic systems which embeds messages into a video stream by changing the parity of 'suitable' D.C.T. blocks.

[207] **'6th ACM International Multimedia Conference (ACM Multimedia'98)'**
ACM, Bristol, England, Sept. 1998. ISBN 1-58113-036-8.

[208] **'Multimedia and Security – Workshop at ACM Multimedia'98'**
J. Dittmann, P. Wohlmacher, P. Horster, R. Steinmetz, Eds., vol. 41 of GMD Report, Bristol, United Kingdom, Sept. 1998. ACM, GMD – Forschungszentrum Informationstechnik GmbH, Darmstadt, Germany.

[209] **'Multimedia Computing and Networking 1997'**
M. Freeman, P. Jardetzky, H. M. Vin, Eds., vol. 3020, San Jose, California, U.S.A., Feb. 1997. The Society for Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIE), SPIE. ISBN 0-8194-2431-5, ISSN 0277-786X.

[210] **'Information Hiding: Second International Workshop'**
D. Aucsmith, Ed., vol. 1525 of Lecture Notes in Computer Science, Portland, Oregon, U.S.A., 1998. Springer-Verlag, Berlin, Germany. ISBN 3-540-65386-4.

[211] **'Computer Security – 5th European Symposium on Research in Computer Security, (ESORICS'98)'**
J.-J. Quisquater, Y. Deswarte, C. Meadows, D. Gollmann, Eds., vol. 1485 of Lecture Notes in Computer Science, Louvain-la-Neuve, Belgium, Sept. 1998. Springer, Berlin, Germany. ISBN 3-540-65004-0.

4.6 Information hiding into other covers

[212] **'Mimic Functions'**
P. Wayner, Cryptologia, vol. XVI no. 3 pp. 193–214, July 1992 , .
The author shows how the inverse of Huffman coding can be used to endow one file with the statistical characteristics of another. Examples are given of randomly generated text with the statistical properties of English, for third order through sixth order statistics and for a context free grammar.

[213] **024122**, **'Anti-counterfeit trials begin with watermark technology'**
Financial Technology International Bulletin, vol. 9 no. 2 pp. 6–7, Oct. 1993 , .
VISA is beginning trials of watermark magnetic strip technology with 30,000 cards in Nottingham, UK. This technology embeds a unique serial number in the magnetic strip to make counterfeiting hard; it is already in use in Sweden.

[214] **032134**, **'Visual Cryptography'**
A. S. M Naor, in Eurocrypt 94, Perugia, Italy, 9–11 May 1994, Lecture Notes in Computer Science, pp. 1–12, Springer-Verlag.
The authors show that visual information can be protected in such a way that it can be decoded using the human eye rather than by a computer. They hide pictures by

splitting them into seemingly random patterns of dots: when these are superimposed, the picture appears. The technique has perfect secrecy (in Shannon's sense), and can be used to hide signatures on ID cards so that they are only legible through a special filter. It can also be generalised to a k out of n secret sharing scheme (for small k and n).

[215] **042160**, **'Rechnergestützte Steganographie: Wie sie Funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist'**
S. Möller, A. Pfitzmann, I. Stierand, Datenschutz und Datensicherung, vol. 18 no. 6 pp. 318–326, 1994 , .
The authors describe a steganography program called DigiStilz which hides ciphertext or other material in the least significant bits of a digital (ISDN) telephone conversation. It is keyed in that the distance between two ciphertext bits is determined by a pseudorandom number, and transmission is blanked when the speech volume drops below a threshold. They tabulate test results; the rate at which the presence of ciphertext could be detected by ear varied from 1 bit in 8 for a noisy background to 1 in 64 for a quiet one. They argue that the ease with which such a system can be implemented makes legal controls on cryptography pointless.

[216] **053105**, **'Protecting ownership rights through digital watermarking'**
H. Berghal, L. O'Gorman, IEEE Computing, vol. 29 no. 7 pp. 101–103, July 1996 , .
The authors discuss the use of both visible and invisible watermarks to protect pictures, text and other intellectual property.

[217] **054120**, **'Fractal Based Image Steganography'**
P. Davern, M. Scott, in Anderson [402], pp. 279–294.
The authors present an information hiding scheme based on fractal compression techniques. The key consists of two non-overlapping regions of the image, selected by the user; the image is then subjected to fractal compression, and message bits of 1 and 0 cause the compression software to use templates in the two key regions respectively.
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[218] **054125**, **'Computer Based Steganography: how it works and why therefore any restriction on cryptography are nonsense, at best'**
E. Franz, A. Jerichow, S. Möller, A. Pfitzmann, I. Stierand, in Anderson [402], pp. 7–21.
The authors discuss a system for hiding ciphertext in the low order bits of an ISDN telephone signal, and report measurements of the perceptibility of various covert signal levels as a function of the cover signal and background noise. They also discuss the meaning of perfect and pragmatic security in the stego context. They argue that steganography is easy, and thus restrictions on crypto will simply force criminals to use stego which will make the law enforcement job harder.
<http://www.semper.org/sirene/publ/FJMP_96Stego.ps.gz>.

[219] **054140**, **'Steganography for DOS Programmers'**
A. Johnson, Dr. Dobb's journal of software tools, no. 261 pp. 48–51, Jan. 1997 , .
The author discusses hiding ciphertext between the end of a file and the end of the last block it uses on disk; he provides source code to do this in DOS.

[220] **061105**, **'Challenges for copyright in a digital age'**
I. D. Bramhill, M. R. C. Sims, BT Technology Journal, vol. 15 no. 2 pp. 63–73, Apr. 1997 , .
The authors talk about copyright management technology, including DVD and watermarking; they suggest binding licensed content to machine characteristics such as hardware configuration, bad disk sectors and the file system structure.

[221] **072138**, **'Watermarking Three-Dimensional Polygonal Models Through Geometric and Topological Modifications'**

R. Ohbuchi, H. Masuada, M. Aono, IEEE Journal on Special Areas in Communications, vol. 16 no. 4 pp. 551–560, May 1998 , .
Three techniques for hiding information in 3D-polygonal models are presented. They use embedding primitives which are invariant to various geometric transformations. The first two techniques modify dimensionless quantity pairs such as ratios of triangles or ratios of the volumes of a pair of tetrahedrons. The third one, which is visible when the model is displayed using wire-frame, changes the density of the triangles of the polygonal mesh.

[222] **073154**, **'Opportunities for Watermarking Standards'**
F. Mintzer, G. W. Braudaway, A. E. Bell, Communications of the A.C.M., vol. 41 no. 7 pp. 57–64, July 1998 , .
The authors suggest that certain watermarking applications like the software interfaces should be standardised. They also recommend to define a benchmark set of watermarking attacks by which watermarking robustness could be judged.

[223] **073184**, **'In Business Today and Tomorrow'**
J. Zhao, E. Koch, C. Luo, Communications of the A.C.M., vol. 41 no. 7 pp. 67–72, July 1998 , .
The paper reviews various uses of digital watermarking technology including banking, defence and copyright marking. The authors argue that this technology has very promising applications and that existing systems can be tremendously improved.

[224] **074154**, **'Watermarking Multiple Object Types in Three-Dimensional Models'**
R. Ohbuchi, H. Masuda, M. Aono, in Dittmann et al. [405], pp. 83–91.
This is a short version [221].

[225] **'Geometry-Based Watermarking of 3D Models'**
O. Benedens, IEEE Computer Graphics and Applications, vol. 19 no. 1 pp. 46–55, Jan. / Feb. 1999 , .
Watermarks embedded in 3D models should be robust at least against mesh simplification. The author presents an alternative method which fills this requirements at the cost of *a priori* data needed for extraction. The embedding is done by moving the center of mass of particular set of vertices.

[226] **'Watermarking 3D Objects for Verification'**
B.-L. Yeo, M. M. Yeung, IEEE Computer Graphics and Applications, vol. 19 no. 1 pp. 36–45, Jan. / Feb. 1999 , .
The authors present a watermarking algorithm to detect modification or tampering of 3D objects. They also introduce a framework for such kind of digital watermarking.

[227] **'Fingerprinting Digital Circuits on Programmable Hardware'**
J. Lach, W. Mangione-Smith, M. Potkonjak, in Aucsmith [369], pp. 16–31.
The authors discuss how to embed copyright marks in chip designs that are implemented in field programmable gate arrays by choosing from alternate but equivalent implementations of the same Boolean function in the configurable logic blocks which are the primitive elements of these devices. The design is subdivided into logical 'tiles' each with (say) 8 equivalent implementations, and in these are encoded a copyright mark which has been subjected to public key encryption and error control coding.
<http://www.icsl.ucla.edu/~jlach/info_hiding_final.ps>.

[228] **'On Software Protection via Function Hiding'**
T. Sander, C. F. Tschudin, in Aucsmith [369], pp. 111–123.
The authors discuss means of protecting software by allowing the execution of encrypted functions. The idea is to compute a polynomial function such as a checksum which is hidden behind Goldwasser-Micali encryption, and is more efficient

than previous constructions such as that of Abadi and Feigenbaum.
`<http://www.icsi.berkeley.edu/~sander/publications/hiding.ps>`.

[229] **'Information Hiding to Foil the Casual Counterfeiter'**
D. Gruhl, W. Bender, in Aucsmith [369], pp. 1–15.
The authors present a marking method to prevent people from printing bank notes on usual high quality ink jet printers. The marking method itself uses the "patch work" algorithm (**054106**) with large random patches. A technique called "tartan threads" is used to help the detection by the printer which should stop printing before the end of the image.

[230] **074117**, **'Audio and optical cryptography'**
Y. Desmedt, S. Hou, J. Quisquater, in International Conference on the Theory and Applications of Cryptology and Information Security, Beijing, China, 18–22 Oct. 1998, number 1514 in Lecture Notes in Computer Science, pp. 392–404. ISBN 3-540-65109-8.
This paper presents two new cryptographic schemes which make use of the wave properties of sound and light. Both are secret sharing schemes in which shares are music or images and guarantee perfect secrecy their high quality also prevents detection by a human censor. Reconstruction depends on their combination. For example, information may be coded by the apparent direction of a source on stereophonic sound, with the channels being the shares.

[231] **'Cerebral Cryptography'**
Y. G. Desmedt, S. Hou, J.-J. Quisquater, in Aucsmith [369], pp. 62–72.
A steganographic system based on stereoscopy. The method is based on secret sharing, but the two secret images are not random, and so less suspicious than the shares obtain with visual cryptography (**032134**). The decoding simply uses a stereoscope.

[232] **'The Steganographic File System'**
R. J. Anderson, R. M. Needham, A. Shamir, in Aucsmith [369], pp. 73–82.
The authors present a steganographic file system. This is a storage mechanism designed to give the user a very high level of protection against being compelled to disclose its contents. It will deliver a file to any user who knows its name and password; but an attacker who does not possess this information and cannot guess it, can gain no information about whether the file is present, even given complete access to all the hardware and software.

[233] **'Soft Tempest: Hidden Data Transmission using Electromagnetic Emanations'**
M. G. Kuhn, R. J. Anderson, in Aucsmith [369], pp. 124–142.
The authors discuss techniques that enable the software on a computer to control the electromagnetic radiation it transmits. This can be used for both attack and defence. To attack a system, malicious code can encode stolen information in the machine's RF emissions and optimise them for some combination of reception range, receiver cost and covertness. To defend a system, a trusted screen driver can display sensitive information using fonts which minimise the energy of these emissions.

[234] **'Information Hiding: Second International Workshop'**
D. Aucsmith, Ed., vol. 1525 of Lecture Notes in Computer Science, Portland, Oregon, U.S.A., 1998. Springer-Verlag, Berlin, Germany. ISBN 3-540-65386-4.

[235] **'Information hiding: first international workshop'**
R. J. Anderson, Ed., vol. 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, May 1996. Springer-Verlag, Berlin, Germany. ISBN 3-540-61996-8.
This workshop on information hiding formed part of a six month research

programme which was held in 1996 at the Isaac Newton Institute on Computer Security, Cryptography and Coding Theory.
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[236] **'Multimedia and Security – Workshop at ACM Multimedia'98'**
J. Dittmann, P. Wohlmacher, P. Horster, R. Steinmetz, Eds., vol. 41 of GMD Report, Bristol, United Kingdom, Sept. 1998. ACM, GMD – Forschungszentrum Informationstechnik GmbH, Darmstadt, Germany.

5 Electronic copyright management systems

[237] **'A WWW service to embed and prove digital copyright watermarks'**
J. Zhao, in European Conference on Multimedia Applications, Services and Techniques, Louvain-la-Neuve, Belgium, May 1996, pp. 695–710.
The author presents an on-line registration service for image watermarking using the Web. The user just has to send the URL of the image he wants to watermark. Then the watermarking service (based on SysCoP [125]) returns a pointer to the watermarked image.
<http://www.crcg.edu/˜jzhao/pub.html>.

[238] **'A Copyright Protection Environment for Digital Images'**
A. Perrig Diploma dissertation, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, Feb. 1997.
The author reviews various risks involved in watermarking technology and suggests some attacks such as the use of a watermark detector as an oracle to compute an 'unwatermarked' object. The author then proposes a watermarking environment which involves various cryptographic protocols between the copyright holder, the copyright office, the buyer and a certification agency.

[239] **064191**, **'The Secure Distribution of Digital Contents'**
E. van Faber, R. Hammelrath, F. P. Heider, in 13th Annual Computer Security Application Conference, San Diego, California, 8–12 Dec. 1997, pp. 16–22, IEEE Computer Society. ISBN 0-8186-8274-4.
The paper describes an infrastructure to distribute digital goods. The digital contents are distributed encrypted, and customers after having paid for the goods can obtain the decryption key from a trusted centre. Customers must be registered with an authorisation centre that performs the access control mechanisms.

[240] **072101**, **'A Java-based platform for intellectual property protection on the World Wide Web'**
T. J. Alexandre, Computer Networks and ISDN Systems, vol. 30 no. 1–7 pp. 591–593, 1998 , .
This note describes a project to encapsulate digital content in Java based objects that decode it on receipt of payment.

[241] **073101**, **'How Watermarking Adds Value to Digital Content'**
J. M. Acken, Communications of the ACM, vol. 41 no. 7 pp. 75–77, July 1998 , .
The author explains that the content protection methods must be scalable so they match the value of the content. In fact each application has its own requirements. More generally, hidden add value to the content, for instance, accountancy audit trails can be hidden in images.

[242] **073152**, **'The 'Ticket' Concept for Copy Control Based on Embedded Signalling'**
J.-P. M. G. Linnartz, in Quisquater et al. [251], pp. 257–274.
The author explains the technical requirements for the DVD marking project and

Phillips' proposed solution. The copy control marks ('free copy', 'copy never', 'one copy' and 'copy no more') are implemented using a 'ticket' which is typically a physical marker associated with the data but stored in locations that are not writable by normal hardware products. An example is the groove wobble in optical discs which can only be inserted in a disc at the time it is pressed. Copy control involves comparing the value of successive hashes of the ticket to the watermark.

[243] **073153**, **'Protecting Digital Media Content'**
N. Memom, P. W. Wong, Communications of the ACM, vol. 41 no. 7 pp. 35–43, July 1998 , .
The authors explain the basic principles of digital watermarking and show various applications through a set of selected examples (including **071112**, **043125**, **063160**, **043167**). They conclude that robust watermarking is a non-trivial problem for which no general solution exists.

[244] **073404**, **'DHWM: A Scheme for Managing Watermarking Keys in the Aquarelle Multimedia Distributed System'**
D. Augot, J.-F. Delaigle, C. Fontaine, in Quisquater et al. [251], pp. 241–255.
This paper presents a protocol and architecture that uses watermarking technology with key management based on the Diffie-Hellman key exchange and a trusted third party (TTP). The key created by the copyright owner and the TTP is used to parameterise the watermarking function. Since the image is watermarked by the owner, no image is exchanged on the network and there is no need for encryption – which complies with current French regulations.

[245] **074130**, **'Copyright and Content Protection for Digital Images based on Asymmetric Cryptographic Techniques'**
A. Herrigel, S. Voloshynovskiy, in Dittmann et al. [405], pp. 99–112.
The authors present a full copyright protection system: watermarking and registration protocols. They show how one can address the legal aspects of the problem using public key cryptography and signatures. They do not assume Internet connection for their protocols since artists usually want to protect high quality images, typically 7 to 10 Mb. All registration requests are de facto proceeded. Timestamps make the difference in case of problem. Certification is based on X509 with 4096 bit keys.

[246] **074352**, **'Digital Content & Intellectual Property Rights'**
A. Ramanujapuram, P. Ram, Dr Dobb's, no. 292 pp. 20–27, Dec. 1998 , .
The authors present solutions to combat intellectual property rights violations developed at Xerox, Palo Alto. This includes a language that can be used to specify rights for digital works and active document objects containing encrypted content, rights labels, watermarks and active control, rights authorisation service, payment system and right management platform for transaction.

[247] **'Intellectual property protection systems and digital watermarking'**
J. Lacy, S. R. Quackenbush, A. R. Reibman, J. H. Snyder, Optics Express, vol. 3 no. 12 pp. 478–484, 7 Dec. 1998 , .
The authors discussed what features an intellectual protection system should possess, with particular emphasis on persistent labelling via watermarking. Three different watermarking mechanisms applicable to compressed media were described and an example of watermarking integrated with MPEG-2 Advanced Audio Coder was given.

[248] **'Secure Copyright Protection Techniques for Digital Images'**
A. Herrigel, J. J. K. Ó Ruanaidh, H. Petersen, S. Pereira, T. Pun, in Aucsmith [369], pp. 169–190.
A full copyright protection environement is presented. The authors first detail a set of basic cryptographic algorithms based on an X.509 public key infrastructure for

registering and trading images. Then, they overview a rotation and scale invariant public watermarking system (see also **073162**). To improve further the robustness of the method, a "template" is embedded together with the data, making the detection of possible distortion easier. Robustness is evaluated with respect to rotation, scaling, cropping, JPEG and noise addition.

[249] **'Protecting Digital-Image Copyrights: A Framework'**
G. Voyatzis, I. Pitas, IEEE Computer Graphics and Applications, vol. 19 no. 1 pp. 18–24, Jan./Feb. 1999 , .
In this journal version of their previous paper (see **074160**), the authors extend a list of intentional attacks against digital watermarking systems concluding that robustness to geometrical distortions is an essential remaining problem.

[250] **'Information Hiding: Second International Workshop'**
D. Aucsmith, Ed., vol. 1525 of Lecture Notes in Computer Science, Portland, Oregon, U.S.A., 1998. Springer-Verlag, Berlin, Germany. ISBN 3-540-65386-4.

[251] **'Computer Security – 5th European Symposium on Research in Computer Security, (ESORICS'98)'**
J.-J. Quisquater, Y. Deswarte, C. Meadows, D. Gollmann, Eds., vol. 1485 of Lecture Notes in Computer Science, Louvain-la-Neuve, Belgium, Sept. 1998. Springer, Berlin, Germany. ISBN 3-540-65004-0.

[252] **'Multimedia and Security – Workshop at ACM Multimedia'98'**
J. Dittmann, P. Wohlmacher, P. Horster, R. Steinmetz, Eds., vol. 41 of GMD Report, Bristol, United Kingdom, Sept. 1998. ACM, GMD – Forschungszentrum Informationstechnik GmbH, Darmstadt, Germany.

6 Steganalysis and other attacks

[253] **063115**, **'Can invisible watermark resolve rightful ownerships?'**
S. Craver, N. Memon, B.-L. Yeo, M. M. Yeung, in Sethin, Jain [271], pp. 310–321.
The authors present a protocol attack on watermarking systems and apply it to NEC system (a private marking system [129]) and to Pitas' method (public marking method [134]). The attack relies on the fact that if two different watermarks are present on the same document then it is not possible to say who is really the owner unless modifying the existing schemes. This leads to a discussion on the usefulness of digital watermarks for ownership identification.

[254] **'Public watermarks and resistance to tampering'**
I. J. Cox, J.-P. M. G. Linnartz, in International Conference on Image Processing (ICIP'97), Santa Barbara, California, U.S.A., 26–29 Oct. 1997, IEEE. ISBN 0-8186-8183-7.
The authors present different general and possible attacks on watermarking systems. The first one exploits the presence of a watermark detector device and explore pixel-by-pixel an image at the boundary where the detector change from 'absent' to 'present'. The author claim that the cost is $O(N)$. A second attack uses the presence of a wartermark inserter and the fact that watermarks of similar images are similar. Other attacks include statistical averaging and a specific attack on copy contro mechanisms embedded in DVDs.
<<ftp://ftp.nj.nec.com/pub/ingemar/papers/icip97.ps>>.

[255] **072113**, **'Some General Methods for Tampering with Watermarks'**
I. J. Cox, J.-P. M. G. Linnartz, IEEE Journal of Selected Areas in Communications, vol. 16 no. 4 pp. 587–593, May 1998, Special issue on copyright & privacy protection.
The authors propose some very general attacks on copy protection mechanisms

such as those used in DVD. For instance, they show how one can use a watermark detector as an oracle to construct an unwatermarked copy.
<ftp://ftp.nj.nec.com/pub/ingemar/papers/jsac98.zip>.

[256] **072114**, **'Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications'**
S. Craver, N. Memon, B.-L. Yeo, M. M. Yeung, IEEE Journal of Selected Areas in Communications, vol. 16 no. 4 pp. 573–586, May 1998, Special issue on copyright & privacy protection.
Many marking schemes are linear, in that an image I and a mark M give a marked image $I + M$. This means that an attacker whose mark is M' can claim that the image is his and the original unmarked image was $I + M - M'$. This means that the rightful owner cannot prove ownership. The author gives practical examples of this attack, and proposes some remedies, such as non-invertibility and quasi-invertibility of the watermarking mechanism.

[257] **073119**, **'Technical Trials and Legal Tribulations'**
S. Craver, B.-L. Yeo, M. Yeung, Communications of the ACM, vol. 41 no. 7 pp. 44–54, July 1998 , .
The authors present and classify the inadequacies and limitations imposed by watermarking schemes from the insertion of a watermark to its interpretation. They also examine the roles and expectation of the different parties involved. Finally the recognise four classes of attacks, namely robustness, presentations, interpretation and legal attacks, for each of which detailed examples are given.

[258] **073147**, **'Removing Spatial Spread Spectrum Watermarks by Non-linear Filtering'**
G. C. Langelaar, R. L. Lagendijk, J. Biemond, in 9th European Signal Processing Conference (EUSIPCO'98), Island of Rhodes, Greece, 8–11 Sept. 1998, pp. 2281–2284. ISBN 960-7620-05-4.
The authors notice that a 3x3 median filter seems to be the best way to separate an image from the spread spectrum watermark it contains. A watermark remover is proposed and experimental results show successful attacks against the schemes of **054106**, **054163** and **063160**.

[259] **074104**, **'Frequency mode L.R. attack operator for digitally watermarked images'**
R. Barnett, D. E. Pearson, Electronics Letters, vol. 34 no. 19 pp. 1837–1839, Sept. 1998 , .
The authors show how one can use the Laplacian transform of an image to attack watermarking systems. In a first attack the new image I' is given by $I' = I - \alpha\nabla^2(\nabla^2 I - I)$ where α is the strength of the attack. Frequency mode Laplacian removal is an improved version of this and introduces 8×8 D.C.T. blocks and γ-correction.

[260] **074107**, **'Results of attacks on a claimed robust digital image watermark'**
G. W. Braudaway, in van Renesse [403].
The author shows the impact of different attacks and manipulations (small-angle rotation, resizing, cropping, sharpening, JPEG compression, tiling, un-correlated noise, overwatermarking) on an invisible watermarking system developed at I.B.M. and presented at ICIP 97. He argues that digital watermarking remains a largely untested field.

[261] **074116**, **'Watermarking: Who Cares? Does it Work?'**
E. J. Delp, in Dittmann et al. [405], pp. 123–137.
The author lists some attacks on marking systems and argues that the proof of ownership problem can indeed be solved using timestamps and not watermarks. The forgery detection can also be done without watermarks: just using 2D hashing

and timestamp. He also argues that watermark have never been tested in court and that Disney *et al.* are not interested in proof of ownership.

[262] **074158**, **'Weaknesses of Copyright Marking Systems'**
F. A. P. Petitcolas, R. J. Anderson, in Dittmann et al. [405], pp. 55–61.
The authors show that the first generation of copyright marking systems does not fulfil the expectation of users through a number of attacks that enable the information hidden by them to be removed or otherwise rendered unusable. They also propose a possible benchmark to compare these systems on a fair basis.

[263] **'Improved robust watermarking through attack characterisation'**
D. Kundur, D. Hatzinakos, Optics Express, vol. 3 no. 12 pp. 485–490, 7 Dec. 1998 , .
The authors described a novel watermarking approach in which a reference watermark is used in addition to a conventional one. The reference watermark is used by the decoder to model the distortion the conventional watermark might have experienced. It is claimed that this can minimise the error probability during watermarking extraction. Simulations show a good effectiveness of this technique.
`<http://epubs.osa.org/oearchive/source/7118.htm>`.

[264] **'Robust Digital Watermark Based on Key-Dependent Basis Functions'**
J. Fridrich, A. C. Baldoza, R. J. Simard, in Aucsmith [369], pp. 143–157.
An attack on **054118** is presented using the fact that areas of a watermarked image can be known to an attacker (e.g. uniform brightness). An enhanced version of **054118**, using a set of general, random, smooth, orthogonal patterns depending on a key, is then presented. Robustness is evaluated with respect to JPEG compression, resampling and filtering.

[265] **'Attacks on Copyright Marking Systems'**
F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, in Aucsmith [369], pp. 218–238.
The authors describe a number of attacks against digital watermarking schemes. The most general attack involves the application of suitably chosen distortion to the object: jitter and resampling in the case of audio, and nonlinear geometrical distortions coupled with noise addition and luminance distortion in the case of images. There is a special attack on echo hiding, techniques whereby an image is broken up into juxtaposed subimages which render to the same picture but foil the mark detector, and some attacks based on protocol issues.

[266] **'Testing Digital Watermark Resistance to Destruction'**
S. Sowers, A. Youssef, in Aucsmith [369], pp. 239–257.
The authors show results of some destruction attacks against publicly available steganographic software.

[267] **'Analysis of the Sensitivity Attack Against Electronic Watermarks in Images'**
J.-P. M. G. Linnartz, M. van Dijk, in Aucsmith [369], pp. 258–272.
The authors give an information-theoretical analysis of the oracle attack. Even if the attacker does not know much about the watermark embedding method, he can still use the bit of information returned by the detector (i.e. yes or no) to remove the watermark by applying small changes to the image until the decoder cannot find it anymore. The analysis leads the author to propose a countermeasure to this attack: randomise the detection process. Rather than having only one threshold for the hypothesis testing, two are used. Between the thresholds the detector returns a random value, outside the threshold it returns a correct answer.
`<http://diva.eecs.berkeley.edu/~linnartz/portland.ps.gz>`.

[268] **'Steganalysis of Images Created Using Current Steganography Software'**
N. F. Johnson, S. Jajodia, in Aucsmith [369], pp. 273–289.
The authors introduce "steganalysis," the art of discovering steganographic messages. They show how many publicly available steganographic tools leak information and introduce the groundwork of a tool for automatically detecting the existence of hidden messages in images.

[269] **'Twin Peaks: The Histogram Attack on Fixed Depth Image Watermarks'**
M. Maes, in Aucsmith [369], pp. 290–305.
The authors present an attack to some image watermarks based on histogram analysis. It relies on the fact that histograms of fixed colour depth images is very peaky and adding a $0, 1$ random sequence to them typically splits the peaks into two 'twins'.

[270] **'Information Hiding: Second International Workshop'**
D. Aucsmith, Ed., vol. 1525 of Lecture Notes in Computer Science, Portland, Oregon, U.S.A., 1998. Springer-Verlag, Berlin, Germany. ISBN 3-540-65386-4.

[271] **'Storage and Retrieval for Image and Video Database V'**
I. K. Sethin, R. C. Jain, Eds., vol. 3022, San Jose, California, U.S.A., Feb. 1997. The Society for Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIE), SPIE. ISBN 0-8194-2433-1, ISSN 0277-786X.

[272] **'Optical Security and Counterfeit Deterrence Techniques II'**
R. L. van Renesse, Ed., vol. 3314, San Jose, California, U.S.A., 28–30 Jan. 1998. The Society for Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIE), SPIE. ISBN 0-8194-2556-7, ISSN 0277-786X.

[273] **'Multimedia and Security – Workshop at ACM Multimedia'98'**
J. Dittmann, P. Wohlmacher, P. Horster, R. Steinmetz, Eds., vol. 41 of GMD Report, Bristol, United Kingdom, Sept. 1998. ACM, GMD – Forschungszentrum Informationstechnik GmbH, Darmstadt, Germany.

7 Intellectual property law

[274] **051315**, **'The EPS CD and CD-ROM Security Conference 1995'**
Anonymous, Computer Law and Security Report, vol. 12 no. 1 pp. 28–36, Jan. / Feb. 1996 , .
This article presents summaries of a number of presentations at a conference on the security of software and other intellectual property distributed by CD-ROM. It covers the pros and cons of distributing software in encrypted form, the use of holographic identifiers and digital fingerprinting of images.

[275] **063321**, **'A Right to read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace'**
J. E. Cohen, Connecticut Law Review, vol. 28 pp. 981–1039, 1996 , .
The author points out that many proposed electronic copyright management systems would identify readers and thus remove the current right to read anonymously. She argues that this could contravene the first amendment to the US constitution. Any right to demand the identity of readers is a function of context, and although it applies for restricted circulation material (such as within a club), it does not apply to material offered on general sale. Thus a proposed law that would ban tampering with copyright management systems is unconstitutional.

[276] **064383**, **'Downloading, Information Filtering and Copyright'**
E. Schweighofer, Information & Communications Technology Law, vol. 6 no. 2, June 1997 , .
This paper reviews legal issues relevant to copyright and document management, filtering and other issues. Digital watermarking, encryption and other technical issued are also briefly mentioned.

[277] **'Copyright Theft'**
J. Gurnsey, Aslib Gower, Aldershot, England, 1995. ISBN 0-566-07631-4.
This book, which reviews the main abuses of copyright law, raises more questions

than it supplies answers. This truly reflects the current state of copyright law: lagging well behind the technology. After a brief but fairly complete history of the copyright law and the associated theft, the author details existing countermeasures, emphasising the international issues and clarifying many common misconceptions. The main part of the book explores the effect of copyright abuse on the print publishing and recording industries: statistics help understand the evolution and the global distribution of piracy. One lesson learned is that the technical capability of copyright thieves should not be underestimated. The book also explores: databases, software, digital broadcasting and video issues; it shows the inefficiency of current international conventions in this domain and the implications for developing countries. The conclusion is that without effective management and fair protection, new technologies will fail to meet their full potential; the risk is a 'sterile society in which the creative process is stifled.'.

[278] **072121**, **'Forensic Copyright Protection'**
D. Grover, The Computer Law and Security Report, vol. 14 no. 2 pp. 121–122, Mar. / Apr. 1998 , .
The article discusses the use of steganography in copyright protection.

[279] **074155**, **'Digital watermarks as a form of copyright protection'**
T. Page, The Computer Law and Security Report, vol. 14 no. 6 pp. 390–392, Nov.–Dec. 1998 , .
The author explains how digital watermarks can be used to reduce illegal copying and track infringers. He argues that the wide spread of digital watermarks together with law preventing removal of the marks will enable right holders to enforce their intellectual property rights.

[280] **074365**, **'COPEARMS and ERMS: safeguarding intellectual property rights in the digital age'**
J. Watkins, Computer Networks and ISDN Systems, vol. 30 no. 16–18 pp. 1589–1595, 1998 , .
The author describes the European Commission sponsored project COPEARMS (Co-ordinating Project for Electronic Authors' Rights Management Systems) and discusses the ERMS (Electronic Right Management System).

[281] **074367**, **'Requirements and Mechanisms of IT-Security Including Aspects of Multimedia Security'**
P. Wolhmacher, in Dittmann et al. [405], pp. 11–19.
The author reviews the basic security mechanisms: confidentiality, integrity, authenticity, etc. She gives the definitions of these as well as some protocols and concludes by asking which of these can be applied to Multimedia.

[282] **'Multimedia and Security – Workshop at ACM Multimedia'98'**
J. Dittmann, P. Wohlmacher, P. Horster, R. Steinmetz, Eds., vol. 41 of GMD Report, Bristol, United Kingdom, Sept. 1998. ACM, GMD – Forschungszentrum Informationstechnik GmbH, Darmstadt, Germany.

8 Fingerprinting & traitor tracing

[283] **'Fingerprinting'**
N. R. Wagner, in Symposium on Security and Privacy, Oakland, California, U.S.A., 25–27 Apr. 1983, Technical Commitee on Security & Privacy, IEEE Computer Society, pp. 18–22.
The author presents a taxonomy of fingerprinting techniques and gives several examples of their use. This lead him to present a statistical fingerprinting method. Finally several other, somewhat more subtle, examples are presented.

[284] **033159**, **'A Holder Verification Protocol Using Fingerprints'**
S. Ozaki, T. Matsumoto, H. Imai, in Korea-Japan Joint Workshop on Information Security and Cryptology, Seoul, Korea, 24–26 Oct. 1993, pp. 1–9.
The authors provide a protocol whereby a personal portable intelligent device with a built-in fingerprint sensor can prove the proper holder's identity to an external verifier without revealing the actual fingerprint.

[285] **034127**, **'Tracing Traitors'**
A. Fiat, in Crypto'94, Santa Barbara, California, U.S.A., 22–25 Aug. 1994, vol. 839 of Lecture Notes in Computer Science, pp. 257–270.
In satellite TV applications, a rogue user might leak either the key or the plaintext of an encrypted broadcast to a pirate audience; the operator will try to track such users by giving each user a personal decryption key with which he can decrypt a session key from an enabling block; thus pirate decoders can be traced. However, an attacker might take several subscriptions and try to generate an innocuous personal key from them; the author discusses various combinatorial schemes which can be used to prevent this.

[286] **044805**, **'Collusion-Secure Fingerprinting for Digital Data'**
D. Boneh, J. Shaw, in 15th Annual International Cryptology Conference, Santa Barbara, California, U.S.A., 27–31 Aug. 1995, number 963 in Lecture Notes in Computer Science, pp. 452–465. ISBN 3-540-60221-6.
The authors define a c-frameproof code to be one such that the only codewords in the feasible set of a coalition of up to c users are the codewords of members of the coalition. They show that for $l = 16c^2 \log n$, there exists an (l, n) error correcting code that is c-frameproof. None of these codes is completely secure against the possibility that colluding attackers could generate a string that was not a codeword; however, if a small probability of error is introduced, some security properties can be established. The size of collusions must be at most the logarithm of the number of users n, and codes of length $\log^6 n$ are constructed.

[287] **053630**, **'Asymmetric Fingerprinting'**
B. Pfitzmann, M. Schunter, in Eurocrypt'96, Saragossa, Spain, 12–16 May 1996, number 1070 in Lecture Notes in Computer Science, pp. 84–95.
A scheme is presented which enables a digital object to be fingerprinted with a mark that is generated jointly by the copyright owner and the licensee. The resulting fingerprint is a signature in the sense that it could only have been generated with the assistance of the licensee, thus offering the owner a non-repudiation service.

[288] **054137**, **'Scalable Document Fingerprinting'**
N. Heintze, Second Usenix Workshop on Electronic Commerce, pp. 191–200, 1996 , .
The author describes a system, Koala, that looks for plagiarism and copyright violation on the net using search engine techniques. The problem is to find documents that are minor edits or reorganisations of an original; the solution is to use fingerprints consisting of a few selected substrings from each document. Postscript is coverted to lower-case ascii and vowels are dropped before choosing strings whose first five letters occur infrequently.

[289] **054447**, **'Modeling Cryptographic Protocols and Their Collusion Analysis'**
S. H. Low, N. F. Maxemchuk, in Anderson [402].
The authors present a model for analysing failures in crypto protocols due to collusion among two or more of the participants. This is motivated by previous work in electronic payment systems where one wants to prove that a certain number of principals need to collude in order to breach a cardholder's privacy. The basic idea is to examine the structure of collusion paths and thus identify which combinations of initial knowledge suffice for an attack. This saves the effort

of exploring a large state transition system.
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[290] **054622**, **'Trials of Traced Traitors'**
B. Pfitzmann, in Anderson [402], pp. 49–64.
The author extends **053630** to shows how the traitor tracing scheme of **034127** can be adapted to add practical non-repudiation properties. The user chooses a random identity and signs a one-way hash of it; the content provider stores this signature in case of future disputes and inputs the random identity into the traitor tracing scheme. This system may be made frameproof by multiparty computation techniques.
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[291] **054625**, **'Blind Decoding, Blind Undeniable Signatures, and Their Applications to Privacy protection'**
K. Sakurai, Y. Yamane, in Anderson [402], pp. 257–264.
The authors adapt blind signature techniques to undeniable signatures and to blind decoding. They suggest the latter mechanism might be used by a publisher whose customers wish to buy pages of information without the publisher learning which pages are of interest; the publisher encrypts them using a given public key, whose corresponding decryption function he will perform for a fixed price. Pages can be blinded before decryption.
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[292] **062147**, **'Anonymous Fingerprinting'**
B. Pfitzmann, M. Waidner, in Eurocrypt'97, Konstanz, Germany, 11–15 May 1997, vol. 1233 of Lecture Notes in Computer Science, pp. 88–102, Springer-Verlag. ISBN 3-540-62975-0.
The authors present protocols whereby customers can buy information anonymously but the anonymity is escrowed, so that if they later resell the information illegally they can be traced. The protocols are more constructive proofs of existence than practical schemes.

[293] **062148**, **'Asymmetric Fingerprinting for Larger Collusion'**
B. Pfitzmann, M. Waidner, in 4th ACM Conference on Computer and Communications Security, Zürich, Switzerland, 1–4 Apr. 1997, pp. 151–160, ACM. ISBN 0-89791-912-2.
The authors present asymmetric fingerprinting and traitor-tracing schemes based on random codes that tolerate collusion by a significant number of traitors. A version of a traitor-tracing scheme using a secure 2-way protocol is also presented. For each scheme the security offered to each party involved in the scheme is examined.

[294] **064193**, **'A Secure Code for Recipient Watermarking against Conspiracy Attacks by all Users'**
H. Watanabe, T. Kasami, in Information and Communications Security — First International Conference, Beijing, China, 11–14 Nov. 1997, number 1334 in Lecture Notes in Computer Science, pp. 413–423, Springer-Verlag. ISBN 3-540-63696-X.
The authors propose a variant on the traitor tracing method of **044805**; the idea is to embed shorter codes but more often.

[295] **073122**, **'Anonymous fingerprinting of electronic information with automatic identification of redistributors'**
J. Domingo-Ferrer, Electronics Letters, vol. 34 no. 13 pp. 1303–1304, 1998 , .
The author suggests a modification of the Pfitzmann-Waidner anonymous fingerprinting scheme (**062147**) which removes the need for help from the registration authority during an illegal copy investigation.

[296] **073136**, **'Fingerprint Image Enhancement: Algorithm and Performance Evaluation'**
L. Hong, Y. Wan, A. Jain, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20 no. 8 pp. 777–789, Aug. 1998 , .
The authors present an algorithm for improving the clarity of ridge and valley structures and suggest its incorporation in minutae extraction routines. An improvement in fingerprint verification performance is also discussed.

[297] **073415**, **'A Mix-Mediated Anonymity Service and Its Payment'**
E. Franz, A. Jerichow, in Fifth European Symposium on Research in Computer Security, Louvain-la-Neuve, Belgium, 16–18 Sept. 1998, vol. 1485 of Lecture Notes in Computer Science, pp. 313–327, Springer-Verlag.
The problem of providing mix-mediated anonymity service on a commercial basis is discussed. Anonymity could be provided both to the payment sender and to the receiver. The use payment protocols based on tick payments scheme of Pedersen (**061437**) is suggested, and the actual protocols being proposed are outlined. The authors discuss the efficiency and foreseen attacks, as well as transfer of the money between the bank, service users and providers.

[298] **073609**, **'Threshold Traitor Tracing'**
M. Naor, B. Pinkas, in 18th Annual International Cryptology Conference, Santa Barbara, California, 23–27 Aug. 1998, vol. 1462, pp. 502–517, Springer-Verlag.
The authors present a tracing scheme for keys used in pirate decoding. The scheme traces the source of keys of decoders which decrypt with probability greater than a certain threshold. When the threshold is very close to 1, the scheme becomes more efficient.

[299] **'Collusion-Secure Fingerprinting for Digital Data'**
D. Boneh, J. Shaw, IEEE Transactions on Information Theory, vol. 44 no. 5 pp. 1897–1905, Sept. 1998 , .
This is a journal version of [286].

[300] **'Information hiding: first international workshop'**
R. J. Anderson, Ed., vol. 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, May 1996. Springer-Verlag, Berlin, Germany. ISBN 3-540-61996-8.
This workshop on information hiding formed part of a six month research programme which was held in 1996 at the Isaac Newton Institute on Computer Security, Cryptography and Coding Theory.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

9 Low-probability-of-intercept radio and spread spectrum

[301] **'Meteor burst communications protocols – The history and role of computing technology in radio communication via meteor trails'**
Q. G. Campbell Technical Report 246, University of Newcastle upon Tyne, Nov. 1987.
The author introduces the necessary background for Meteor Burst Communications (MBC): definitions, basic theory. He also provides a good overview of the fascinating history behind MBC system developments, including several applications. This leads him to emphasise the important role of programmable microprocessors in the growth of these systems. Large survey of the public literature included.

[302] **'Cryptology and the origins of spread spectrum'**
D. Kahn, IEEE Spectrum, vol. 21 no. 9 pp. 70–80, Sept. 1984 , .
This article describes SIGSALY, the first digital secure telephone, which was used by Roosevelt and Churchill during the war. It used a vocoder with 10 bands of 300 Hz, each sampled for amplitude every 20mS; the digital signal was Vernam encrypted (though since the samples had six levels, the arithmetic was modulo 6). The cables from the scrambling equipment to the users were pressurised and alarmed. Finally, the radio link used an early spread spectrum technique to reduce the likelihood of interception or jamming. One of the inventors of spread specturm was the actress Hedy Lamarr, who obtained a US patent in 1941 on a frequency agile torpedo control system.

[303] **'Spread spectrum systems with commercial applications'**
R. C. Dixon, John Wiley & Sons, Inc., New York, New York, U.S.A., third edition, 1994. ISBN 0-471-59342-7.
Spread spectrum techniques provide a number of benefits, most notably signal hiding, jamming margin, selective addressing, multiple access, interference rejection and high-resolution ranging. For nineteen years, Dixon was the standard reference work on spread spectrum, but was relatively unknown outside a circle of military specialists. Recent advances in integration, as well as a 1985 decision by the FCC to allow commercial use, have led to rapid growth in commercial applications ranging from GPS to digital cellular telephones; Dixon has just rewritten his book to take account of all this. The mechanics of spread spectrum systems can be quite complicated. The basic techniques - direct sequence, frequency hopping and time hopping - are simple enough in concept, but there are many complex tradeoffs between error rate, process gain, chip or hop rate, synchronisation, and the various strategies available to participants and opponents; and the linkage between coding, cryptographic and RF engineering aspects is uniquely complicated. Dixon provides a guide to the underlying theory which should be accessible to a graduate student in either discipline, and goes on to discuss the engineering aspects of satellite uplinks, GPS, military tactical radios and modems, digital cellular radio and vehicle location. There are also hundreds of references which provide a lead into the research literature.

[304] **'Meteor burst communications: theory and practice'**
D. L. Schilling, Ed., Wiley series in telecommunications. Wiley, New York, New York, U.S.A., 1993.
The ionised trails of micrometeors entering the earth's atmosphere reflect radio waves, especially in the low VHF band, and attempts have been made since the 1960's to use this phenomenon for communication. Although the initial interest in the subject faded with the introduction of satellites for the bulk of beyond-line-of-sight communications, meteor burst communications are now used in a number of commercial and military rôles. Their intermittent nature, and the relatively small ground footprint of each trail, make them inherently hard to monitor. This book is the first comprehensive guide to the subject to appear in modern times. Such a guide is welcome, as the subject spans a very wide range of subject matter: from the physics of the meteor trails themselves through the various coding and other techniques which are used to maximise the available channel capacity through to a number of issues arising from practical engineering experience. The context of the book is a US Air Force network in Alaska, which provides backup communications for early warning radars in the event that satellite communications are knocked out.

[305] **'Schutz der Vertraulichkeit des Aufenthaltsorts von Mobilfunkteilnehmern'**
H. Federrath, J. Thees, Datenschutz und Datensicherheit, pp. 338–348, June 1995 , .
The authors describe how direct sequence spread spectrum techniques can be used to make it harder for an eavesdropper to determine the phyical location of a trans-

mitter. Low-probability-of-intercept systems use cryptographic rather than maximal length spreading sequences; a direction finding apparatus would need to do a autocorrelation or crosscorrelation analysis of the sequence in order to select the signal. By comparison, frequency agile systems are relatively easy to intercept. There are a number of other engineering factors which need to be considered when designing anonymous networks, such as computer security measures to protect location information stored in the network, and dummy traffic to preventing active attacks through the network. Call setup is troublesome, particularly when initiated by the mobile station; the most elegant solution involves Rabin's beacons.

[306] **042155**, **'Speakeasy: The Military Software Radio'**
R. J. Lackey, D. W. Upmal, IEEE Communications Magazine, vol. 33 no. 5 pp. 56–61, 1995 , .
The authors describe a US Army project to develop a military radio which uses programmable signal processing to emulate more than 15 existing radios, including GPS, cellular phones, satcom, analogue HF, SINCGARS, HAVE QUICK and low probability of intercept modes. It will operate from 2MHz to 2GHz with interchangeable RF modules and IF digitisation; in addition to software waveform processing, there is also a programmable security processor which emulates the comsec and transec features of five existing crypto devices.

[307] **061459**, **'Code acquisition scheme for frequency hopping radio in channels with fading'**
B. M. Todorović, Electronics Letters, vol. 33 no. 3 pp. 177–179, 30 Jan. 1997 , .
Key management is tricky in low-probability-of-intercept systems, and particularly when a fading channel forces frequent resynchronisation. This paper presents a 3-level scheme to enable frequency hop radios to resynchronise rapidly and calculates the probabilities of false alarm, false lock and false dismissal.

[308] **072135**, **'Chip rate hopping provides low probability of detection for direct sequence signals'**
W. D. McPherson, D. A. Hill, L. Mai, J. S. Wright, Electronics Letters, vol. 34 no. 7 pp. 628–629, 2 Apr. 1998 , .
The authors discuss how to make spread spectrum signals hard for chip rate detectors to find. Their system changes the chip rate with each burst of 5 ms or so; chip rates are pseudorandomly distributed from 9 to 10 MHz. They present both theory and measurements, and conclude that low detectability can be guaranteed by fundamental considerations such as bandwidth and observation time.

[309] **074504**, **'Chaotic Frequency Hopping Sequences'**
L. Cong, S. Songgeng, IEEE Transactions on Communications, vol. 48 no. 11 pp. 1433–1437, Nov. 1998 , .
The authors describe a family of frequency hopping sequences generated by non linear dynamical systems. The non linear one dimensional map is partitioned and, depending in which partition the current point is, the frequency chosen.

10 Covert channels

[310] **'A Cautionary Note on Image Downgrading'**
C. Kurak, J. McHugh, in Computer Security Applications Conference, San Antonio, Texas, U.S.A., Dec. 1992, pp. 153–159.
The authors study how one image can be embedded in another; their concern is identifying the threats posed by downgrading classified satellite images. They give examples of pictures of an aircraft, an airfield, and text, embedded in each other by replacing the four least significant bits of each pixel of the cover picture by

the four most significant bits of the embedded picture. The loaded pictures cannot be distinguished by eye, and the quality of the recovered hidden pictures is acceptable for intelligence purposes. They conclude that manual inspection alone is insufficient to prevent image downgrading being used to leak information.

[311] **'Computer and Network Security'**
J. McHugh, chapter An EMACS Based Downgrader for the SAT, pp. 228–237, IEEE Computer Society Press, 1986.

[312] **'A note on the Confinement Problem'**
B. W. Lampson, Communications of the A.C.M., vol. 16 no. 10 pp. 613–615, Oct. 1973 , .
This paper pointed out the existence of covert channels. These channels arise where a resourse is shared between two entities between which we wish to inhibit communication; for example, a virus attached to a 'SECRET' process might signal classified information down to another virus at 'UNCLASSIFIED' by modulating the CPU load or the position of a disk head.

[313] **'A Guide to Understanding Covert Channel Analysis of Trusted Systems'**
V. Gligor Tech. Rep. NCSC-TG-030, National Computer Security Center, Ft. George G. Meade, Maryland, U.S.A., Nov. 1993, Approved for public release: distribution unlimited.
This is the official NSA guide to the identification and elimination of covert channels in multilevel secure systems. Military multilevel secure systems – at least at the higher levels of evaluation – should limit covert channel bandwidth to about one bit per second. The techniques involved include both channel elimination and noise insertion.

[314] **'Covert Channel Capacity'**
J. K. Millen, IEEE Symposium on Security and Privacy, pp. 60–66, 1987 , .
This is one of the classic papers on calculating the capacity of a covert channel using entropy equations; it shows how information-theoretic properties can also be represented in automata-theoretic terms.

[315] **'The Influence of Delay on an Idealized Channel's Bandwidth'**
I. S. Moskowitz, A. R. Miller, in IEEE Symposium on Security and Privacy, 1992, pp. 63–67.
The authors analyse the relationship between the bandwidth of a covert channel and the underlying queueing parameters.

[316] **'Capacity Estimation and Auditability of Network Covert Channels'**
B. R. Venkatraman, R. E. Newman-Wolfe, in IEEE Symposium on Security and Privacy, Oakland, California, U.S.A., 8–10 May 1995, pp. 186–198. ISBN 0-8186-7015-0.
The authors continue their research into how the type, amount, and timeliness of data traffic on a network can be used to send covert information. They discuss their work in light of Browne's ideas of mode security. An audit threshold is analyzed with respect to the maximal damage due to the above types of covert channels. Further details can be found in the first author's dissertation.

[317] **021114**, **'Breaking the Traditional Computer Security Research Barriers'**
Y. Desmedt, in European Symposium for Research in Computer Security, Toulouse, France, 23–25 Nov. 1992, vol. 648 of Lecture Notes in Computer Science, pp. 125–138, Springer-Verlag. ISBN ISBN 3-540-56246.
This article presents an overview of research in computer and communications security, covering identification, covert channels, threshold schemes and reliability. It argues that future trends will continue to be away from multiuser systems and toward single-user machines, particularly notebooks. In this case, much more secure systems can be built, and cryptology will be the key enabling technology.

[318] **021136**, **'Architectural Implications of Covert Channels'**
N. Proctor, P. Neumann, in 15th National Ccomputer Security Cconference, pp. 28–43.
This paper reviews covert channels: how they occur, what assumptions are needed to ignore them, how to eliminate them from resource allocation algorithms and what the tradeoffs are. It then proposes an architecture for eliminating them and describes a design for a multi-level disk drive using manual allocation. This drive can allow read-down and write-up operations which have no covert channel but still yield adequate performance. The authors argue that building secure operating systems is beyond today's technology, and argue that using single-level processors with a multi-level disk gives maximum assurance at a reasonable cost.

[319] **021148**, **'A Tool for Covert Storage Channel Analysis of the UNIX Kernel'**
D. A. Willcox, S. R. Bunch, in 15th National Ccomputer Security Cconference, pp. 697–706.
The authors describe a tool developed at Motorola to perform a covert storage channel analysis on annotated C source code.It was used to analyse UNIX system source code targeted at a B2 evaluation. As it is automated, it can be used more easily than a shared resource matrix; it reports potential covert channels for manual review. Sixty-five potential covert channels were found in one operating system implementation: they are divided into shared identifiers, resource exhaustion, caches, and direct covert channels, and several of them are discussed.

[320] **021229**, **'The Channel Capacity of a Certain Noisy Timing Channel'**
I. S. Moskovitz, A. R. Miller, IEEE Transactions on Information Theory, vol. IT-38 no. 4 pp. 1339–1343, 1992 , .
A covert timing channel may suffer noise generated by time sharing delays as other users compete for resources. Two strategies for communicating in the presence of this noise are analysed and the resulting channel capacity is determined.

[321] **024130**, **'Laser communications for covert links'**
J. L. Jaeger, R. T. Carlson, Laser Communications, pp. 95–106, 1993 , .
The authors describe a prototype laser communications system built by MITRE and others to replace military line-of-sight RF communications. The devices operate in the infrared; this not only increases the difficulty of detection, but also provides eye safety at all distances. The design is described, and extensive field tests reported: depending on the weather, the link operates at 1,024, 128 or 16Kbps, and at the lowest of these rates, the system can cope with all conditions except for heavy fog or rain. Excellent covertness is claimed.

[322] **054202**, **'Covert Channel Analysis for Stubs'**
M. S. Anderson, M. A. Ozols, in Anderson [402], pp. 95–113.
The authors present a covert channel analysis for the Stubs network security devices developed by DSTO in Australia. The claim is that the use of strong military crypto to seal messages limits an attacker in the 'high' part of the network to manipulating the supply of sealed messages. Seal timestamps limit this manipulation to a short time window. A formal analysis is given of the channel capacity under various attack and noise assumptions. This leaves open the possibility of hidden messages in text that passes human reviewers. They suggest a 'blind man's filter' — a filter that will not pass information (such as minor font changes) if they are such that the human reviewer would not discern them; a suggested technique is OCR scanning.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[323] **054222**, **'Hiding Data in the OSI Network Model'**
T. G. Handel, M. T. Sandford, in Anderson [402], pp. 23–38.
The authors present a systematic analysis of the covert channel capacity of the

OSI network model. Some of the available mechanisms at each of the seven layers are described, and estimates given of the overall bandwidth. They argue that eliminating this covert bandwidth would be an immense task and could only be partially automated.
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[324] **054230**, **'Covert Channels — A Context-Based View'**
C. Meadows, I. Moskowitz, in Anderson [402], pp. 73–93.
The authors propose to classify covert channels according to the context in which they occur rather than the mechanisms that they employ. The main distinction is between low-to-high service, high-to-low service, shared service and incomparable service. The claimed advantage of this method is that covert channels arising in similar contexts can be dealt with in similar ways. Some compositional properties are discussed in the context of the NRL pump.
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[325] **063213**, **'A Multiversion Transaction Scheduler for Centralized Multilevel Secure Database Systems'**
T. F. Keefe, W. T. Tsai, in High-Assurance Systems Engineering Workshop, Niagara on the Lake, Canada, 21–22 Oct. 1996, pp. 206–213, IEEE. ISBN 0-8186-7629-9.
This paper examines the covert channel problems that arise due to the contention caused by concurrent execution of transactions in an MLS DBMS. The authors propose getting around these problems by using multiversion schedulers. An abstract model is developed and shown to satisfy noninterference.

[326] **064168**, **'Using datagram based multimedia streams as a cover channel for hidden transmission'**
A. Patel, N. Schmidt, M. Bessonov, in Third IFIP TC6/TC11 Working Conference on Communications and Multimedia Security, Athens, Greece, 22–23 Sept. 1997, pp. 239–249, Chapman and Hall. ISBN 1-880446-90-1.
A scheme for transmitting covert data over non-reliable multimedia streams is described in which an error control code, together with bit reordering, is used to encode a secret message. Solutions for resolving packet loss and synchronisation problems are suggested.

[327] **'Information hiding: first international workshop'**
R. J. Anderson, Ed., vol. 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, May 1996. Springer-Verlag, Berlin, Germany. ISBN 3-540-61996-8.
This workshop on information hiding formed part of a six month research programme which was held in 1996 at the Isaac Newton Institute on Computer Security, Cryptography and Coding Theory.
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

11 Anonymity & traffic analysis

[328] **'Untraceable electronic mail, return addresses and digital pseudonyms'**
D. Chaum, Communications of the A.C.M., vol. 24 no. 2 pp. 84–88, Feb. 1981 , .
In this classic article, the author introduces mix-nets (anonymous remailers). These decrypt incoming traffic, add or remove padding, reencrypt it and dispatch it in lexicographically ordered batches. Mechanisms are also discussed for anonymised return addresses, digital pseudonyms, blinded certified mail, and the use of a hier-

archy of subnets to provide scalability. The possible application discussed is digital elections.

[329] **'Networks Without User Observability – Design Options'**
A. Pfitzmann, M. Waidner, in Advances in Cryptology – Eurocrypt '85. 1985, vol. 219 of Lecture Notes in Computer Science, Spinger-Verlag.
In normal communication networks, operators and intruders can easily observe when, how much and with whom the users communicate, even if the users employ end-to-end encryption. Once ISDN is used for almost everything, this could becomes a severe threat. There are, however, a number of technical options to keep the recipient and sender (or at least their relationship) unobservable; the authors consider some possible implementations and extensions, and propose some performance and reliability enhancements.

[330] **'The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability'**
D. Chaum, Journal of Cryptology, vol. 1 pp. 65–75, 1988 , .
Keeping confidential who sends which messages, in a world where any physical transmission can be traced to its origin, seems impossible. The solution presented here is based on passing messages round a ring of participants; it is unconditionally or cryptographically secure, depending on whether it is based on one-time-use keys or on public keys, respectively. It can be adapted to address efficiently a wide variety of practical considerations.

[331] **'Security without Identification: Transaction Systems to Make Big Brother Obsolete'**
D. Chaum, Communications of the A.C.M., vol. 28 no. 10, Oct. 1985 , .
By partitioning consumer information into separate unlinkable domains through the use of user-created "digital pseudonyms," the dangers inherent in large-scale automated transaction systems, as currently structured, can be avoided.

[332] **'How to Break the Direct RSA-Implementation of MIXes'**
B. Pfitzmann, A. Pfitzmann, in Advances in Cryptology – Eurocrypt '89. 1989, vol. 434 of Lecture Notes in Computer Science, Springer-Verlag.
MIXes are a kind of anonymous remailer, suggested by David Chaum in 1981. If RSA is used as this cryptosystem directly, i.e. without hashing to destroy the multiplicative structure, the resulting MIXes can be broken by an active attack which is perfectly feasible in a typical environment. The attack does not affect the basic idea of MIXes, provided they are implemented carefully; but it does show that present security notions for public key cryptosystems may not suffice for a system which is to provide a service such as anonymity. We also warn of attacks on further possible implementations of MIXes, and we mention several implementations which are not broken by any attack we know.

[333] **'Unconditional Sender and Recipient Untraceability in Spite of Active Attacks'**
M. Waidner, in Advances in Cryptology – Eurocrypt '89. 1989, vol. 434 of Lecture Notes in Computer Science, Springer-Verlag.
A protocol is described to send and receive messages anonymously using an arbitrary communication network; it is unconditionally secure. This improves a result by Chaum: The DC-net guarantees the same, but on the assumption of a reliable broadcast network. Since unconditionally secure Byzantine Agreement cannot be achieved, such a reliable broadcast network cannot be realized by algorithmic means. The solution proposed here, the DC^{+}-net, uses the DC-net, but replaces the reliable broadcast network by a fail-stop one. By choosing the keys necessary for the DC-net dependently on the previously broadcast messages, the fail-stop broadcast can be achieved unconditionally secure and without increasing the complexity of the DC-net significantly, using an arbitrary communication network.

[334] **'Receipt-Free Mix-Type Voting Schemes'**
K. Sako, J. Kilian, in Advances in Cryptology – Eurocrypt '95, St Malo, France, May 1995, vol. 921 of Lecture Notes in Computer Science, pp. 393–403, Springer-Verlag.
The authors use Chaum's anonymous channel to construct an anonymous voting scheme under which voters cannot prove how they voted and so cannot so easily be bribed or coerced. However each voter can still check that every vote was properly counted.

[335] **032627**, **'Breaking an Efficient Anonymous Channel'**
B. Pfitzmann, in Advances in Cryptology – Eurocrypt '94, Perugia, Italy, 9–11 May 1994, Lecture Notes in Computer Science, pp. 339–348, Page numbers given here refer to preproceedings.
At Eurocrypt'93, Park, Itoh, and Kurosawa presented two efficient designs for an anonymous channel based on Chaum's mix-nets. The idea was to simulate a trusted host for applications like electronic voting with secret inputs and public outputs. Here, the author first identifies a passive attack against both designs that may allow correlation of inputs and outputs, and shows how to avoid this by careful choice of parameters. She then demonstrates an active attack was proposed that completely breaks one of the designs; there may be ways to avoid this attack on the other design by adding counters and redundancy.

[336] **042183**, **'Performance Analysis of a Method for High Level Prevention of Traffic Analysis Using measurements from a Campus Network'**
B. R. Venkataraman, R. E. Newman-Wolfe, in Tenth Annual Computer Security Applications Conference, Orlando, Florida, 5–8 Dec. 1994, pp. 288–297, IEEE Computer Society Press. ISBN 0-8186-6795-8.
The authors investigated the cost of rerouting and padding the University of Florida's network traffic to provide resistance to traffic analysis. They considered the leakage through a covert channel where a '1' was signified by the presence of traffic on the link from node i to node j. Making the traffic spatially neutral thus corresponds to blocking traffic analysis; thus traffic was rerouted and padded to put the same amount of traffic on each link. Doing this perfectly is a hard linear programming problem, so a number of heuristic solutions were tried and measured.

[337] **054105**, **'Practical Invisibility in Digital Communications'**
T. Aura, in Anderson [402], pp. 265–278.
The author discusses some of the problems of information hiding, including synchronising with a cover message which is a stream such digital audio. Where the cover message is a block, such as a digital picture, his technique is to use the Luby-Rackoff construction to embed the hidden bits pseudorandomly throughout the picture. A test implementation using SHA as the underlying primitive is reported.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[338] **054145**, **'Location Management Strategies Increasing Privacy in Mobile Communication'**
D. Kesdogan, H. Federrath, A. Jerichow, A. Pfitzmann, in 12th International Information Security Conference, Samos, Greece, 21–24 May 1996, pp. 39–48, Chapman & Hall. ISBN 0-412-78120-4.
Means to provide secrecy of user location and anonymity to GSM users are discussed. For the former, the authors suggest using a home computer as a trusted device for processing incoming calls. Anonymity is to be achieved either by periodic issuing of pseudonyms or by group pseudonyms; the latter could possibly work better given the structure of GSM.

[339] **054414**, **'MIXes in Mobile Communication Systems: Location Management with Privacy'**
H. Federrath, A. Jerichow, A. Pfitzmann, in Anderson [402], pp. 121–135.
The authors describe the present arrangements for hiding the location of users in GSM type systems, and discuss how they could be improved. One approach is to use remailer networks; here, one must pay attention to the bandwidth limitations on the air link. One can also use multiple names for mobiles. Various combinations of these techniques are discussed together with their tradeoffs.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[340] **054421**, **'Hiding routing information'**
D. M. Goldschlag, M. G. Reed, P. F. Syverson, in Anderson [402], pp. 137–150.
The authors describe an approach to using multiple 'remailers' which they call 'onion routing' (it actually works with proxies for any type of service, not just mail). The idea is that remailers should be stateless; the initiator chooses routes out and back and constructs an 'onion', a set of remailer addresses successively encrypted under the previous remailer's public key, to enable the responder to reply to a message. The message, plus the reply onion, are then successively encrypted under the public keys of the outbound remailers. The approach has been prototyped for http and telnet.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[341] **054431**, **'Anonymous Addresses and Confidentiality of Location'**
I. W. Jackson, in Anderson [402], pp. 115–120.
The author describes how anonymous remailers can be used to process personal location information from active badges. The goal is that each user should be able to control who has access to information about his location; the mechanism is that the remailers forward this information to a server that the user trusts to enforce his security policy. The crypto protocols used in this system are described.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[342] **064437**, **'Fault Tolerant Anonymous Channel'**
W. Ogata, K. Kurosawa, K. Sako, K. Takatani, in Information and Communications Security — First International Conference, Beijing, China, 11–14 Nov. 1997, vol. 1334 of Lecture Notes in Computer Science, pp. 440–444, Springer-Verlag. ISBN 3-540-63696-X.
The authors show how to construct a MIX-net that is resilient against balking or other misbehaviour of half the remailers. It uses a bulletin board to publicise intermediate results; each participant repeatedly decrypts and shuffles a batch of ciphertexts and proves that he has executed the protocol faithfully.

[343] **064452**, **'Anonymous Connections and Onion Routing'**
P. F. Syverson, D. M. Goldschlag, M. G. Reed, in IEEE Symposium on Security and Privacy, Oakland, California, 4–7 May 1997, pp. 44–54. ISBN 0-8186-7828-3.
This paper is an extension of previous work (**054421**, **061439**) on onion routing implementations of rlogin, http and e-mail on Sun Solaris 2.x. Also, an extended vulnerability assessment is presented.

[344] **071407**, **'Anonymity Control in E-Cash Systems'**
G. Davida, Y. Frankel, Y. Tsiounis, M. Yung, in Financial Cryptography: First International Conference, Anguilla, British West Indies, 24–28 Feb. 1997, vol. 1318 of Lecture Notes in Computer Science, pp. 1–16, Springer-Verlag. ISBN 3-540-63594-7.
The authors suggest that e-cash anonymity should be treated as a control parameter, allowing for revocable anonymity and other features. Anonymity control mod-

els — owner tracing and coin tracing — are reviewed and a simplified version of a protocol from **061614** is presented. The concept of 'distress cash' is introduced that uses a covert channel to mark cash released under threat.

[345] **071123**E. Gabber, P. B. Gibbons, Y. Matias, A. Mayer, in Financial Cryptography: First International Conference, Anguilla, British West Indies, 24–28 Feb. 1997, vol. 1318 of Lecture Notes in Computer Science, pp. 17–31, Springer-Verlag. ISBN 3-540-63594-7.
The authors present a solution that automatically creates and manages user login IDs and passwords for accessing websites. The tool protects the true identity of a user, and supports 'anonymous personalised web browsing' that elaborates on Chaum's idea of digital pseudonyms.

[346] **072127**, **'Real-Time Mixes: a Bandwidth-Efficient Anonymity Protocol'**
A. Jerichow, J. Müller, A. Pfitzmann, B. Pfitzmann, M. Waidner, IEEE Journal on Special Areas in Communications, vol. 16 no. 4 pp. 495–509, May 1998 , .
The authors present a technique to extend MIXes for efficient continuous, real-time communication using fixed MIX cascades. They propose three versions: keeping the sender anonymous from the recipients; vice-versa; and both. They explain how their technique can be apply to ISDN by modifying only layer three of the corresponding OSI model. The authors conclude their paper by considering active attacks such as denial of service and billing issues.

[347] **072144**, **'Anonymous Connections and Onion Routing'**
M. G. Reed, P. F. Syverson, D. M. Goldschlag, IEEE Journal on Special Areas in Communications, vol. 16 no. 4 pp. 482–494, May 1998 , .
This is the extended journal version of conference papers **054421**, **061439**, **064444**, **064452** and **071443** on the Navy Labs' Onion Routing system of anonymous remailers.

[348] **072403**, **'Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers'**
M. Abe, in Advances in Cryptology – Eurocrypt '98, Helsinki, Finland, 31 May– 4 June 1998, vol. 1403 of Lecture Notes in Computer Science, pp. 437–447, Springer-Verlag. ISBN 3-540-64518-7.
The author presents a protocol in which mix-servers cooperate with a bulletin board to provide an anonymity service that is demonstrably secure against a threshold of conspirators, and more efficient than many previously proposed.

[349] **073140**, **'Distributed Temporary Pseudonyms: A New Approach for Protecting Location Information in Mobile Communication Networks'**
D. Kesdogan, P. Reichl, K. Junghärtchen, in Fifth European Symposium on Research in Computer Security, Louvain-la-Neuve, Belgium, 16–18 Sept. 1998, vol. 1485 of Lecture Notes in Computer Science, pp. 295–312, Springer-Verlag.
The authors review the concept of temporary pseudonyms as presented in **054145** and discuss using a third party for guaranteeing the pseudonyms, ideally among n different parties. They then discuss pseudonym collision probabilities and present some simulation results.

[350] **'The Design, Implementation and Operation of an Email Pseudonym Server'**
D. Mazières, M. F. Kaashoek, in 5th A.C.M. Conference on Computer and Communications Security (ACM CCS'98), San Francisco, California, U.S.A., 3–5 Nov. 1998, pp. 27–36. ISBN 1-58113-007-4.
The authors describe the experience of maintaining an email pseudonym server. Beyond protecting the identity of participating users, the server was designed to withstand a variety of denial of service attacks.

[351] **'Communication-Efficient Anonymous Group Identification'**
A. De Santis, G. Di Crescenzo, G. Persiono, in 5th A.C.M. Conference on Computer

and Communications Security (ACM CCS'98), San Francisco, California, U.S.A., 3–5 Nov. 1998, pp. 73–82. ISBN 1-58113-007-4.
The authors present a perfect zero-knowledge, anonymous group identification scheme whose security relies on the computational infeasibility of factoring Blum integers. Given m group members and security parameter n, the scheme has communication complexity $\theta(m+n)$ (where previous results achieved only $\theta(mn)$). The authors extend their scheme so as to also allow $t > 1$ member group identification (again improving the communication complexity from previous work).

[352] **'Stop-and-Go MIXes Providing Probabilistic Security In An Open System'**
D. Kesdogan, J. Egner, R. Büschkes, in Aucsmith [369], pp. 83–98.
This article investigates how active attacks on remailer networks can be made more difficult by probabilistic techniques; the central idea is that instead of collecting and shuffling a minimum number of packets, the packets are subjected to random delays with a suitably chosen distribution. Matters that need attention include secure timestamping of the packets to prevent manipulation by the opponent. The security available is calculated using queuing theory.
`<http://www.cl.cam.ac.uk/~fapp2/ihw98/ihw98-sgmix.pdf>`.

[353] **'Biometric yet Privacy Protecting Person Authentication'**
G. Bleumer, in Aucsmith [369], pp. 99–110.
The author discusses the engineering of pseudonymous credentials for use in applications such as driving licenses and credit cards. He presents a suite of protocols which can be used to bind a credential to a tamper resistant device which identifies its holder by biometric means. They use restrictive blind signatures and a new primitive called restrictive cascade signatures, and can provide unconditional unlinkability against coalitions of checkpoint operators.
`<http://www.research.att.com/library/trs/TRs/98/98.1/98.1.1.body.ps>`.

[354] **'Information hiding: first international workshop'**
R. J. Anderson, Ed., vol. 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, May 1996. Springer-Verlag, Berlin, Germany. ISBN 3-540-61996-8.
This workshop on information hiding formed part of a six month research programme which was held in 1996 at the Isaac Newton Institute on Computer Security, Cryptography and Coding Theory.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[355] **'Information Hiding: Second International Workshop'**
D. Aucsmith, Ed., vol. 1525 of Lecture Notes in Computer Science, Portland, Oregon, U.S.A., 1998. Springer-Verlag, Berlin, Germany. ISBN 3-540-65386-4.

12 Theory

[356] **041222**, **'Coding for Noisy Feasible Channels'**
R. J. Lipton, in IEEE-IMS Workshop on Information Theory and Statistics, Alexandria, Virginia, U.S.A., 27–29 Oct. 1994, p. 27, IEEE press.
The author discusses the idea of a feasible channel. This is a channel where encoding / decoding is all in polynomial time, along with some other more minor criteria. These channels might be a realistic class to consider for covert channel analysis.

[357] **041815**, **'The role of information theory in cryptography'**
U. M. Maurer, in Fourth IMA Conference on Cryptography and Coding. 13–15 Dec. 1993, pp. 49–71, IMA.

The author reviews the standard information theoretic results on perfect secrecy, authentication and secret sharing. He also shows how Shannon's bounds on the key size required for perfect secrecy can be overcome given a public randomiser, provided one can assume that the opponent has finite memory. Finally, he discusses the wiretap channel and the information reconciliation techniques used in quantum cryptography.

[358] **043164**, **'Strong Theoretical Steganography'**
P. Wayner, Cryptologia, vol. XIX no. 3 pp. 285–299, July 1995 , .
The author proposes a system of steganography based on context free grammars. Learning a van Wijngaarden grammar is equivalent to a Turing machine. In a practical system, input ciphertext bits can be used to select productions from the grammar, and can be recovered through parsing so long as the grammar is unambiguous. An example is given based on English text generated using these ideas.

[359] **054119**, **'Surmounting the Effects of Lossy Compression on Steganography'**
C. E. I. D L Currie, in 19th National Information Systems Security Conference, Baltimore, Maryland, 22–25 Oct. 1996, pp. 194–201, NIST.
The effects of the JPEG compression to image-based steganographic information hiding are described. Simplistic information hiding schemes do not work, as the lower four bits are heavily modified and information encoded in them would be corrupted. Information can still be encoded by manipulating pixel colour; but the scheme they used allowed only 30% bit recovery of the embedded data.

[360] **054163**, **'Modulation and Information Hiding in Images'**
J. R. Smith, B. O. Comiskey, in Anderson [402], pp. 207–226.
The authors develop a theory of information hiding in images that sets out to quantify channel capacity and jamming margin. They describe test implementations of information hiding schemes inspired by both direct sequence and frequency hopping spread spectrum concepts. Their relative advantages are discussed; the latter is superior perceptually and has better resistance to accidental removal by compression techniques, while the former is more robust against deliberate removal attempts. They predict a co-evolutionary arms race with compression techniques.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[361] **061811**, **'Towards Characterizing When Information-Theoretic Secret Key Agreement Is Possible'**
U. Maurer, S. Wolf, in International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, 3–7 Nov. 1996, vol. 1163 of Lecture Notes in Computer Science, pp. 196–209, Springer-Verlag.
The authors consider the problem of establishing a secret key between A and B over an insecure channel, where information of an eavesdropper E would be arbitrarily small. For random variables X, Y, and Z, known to A, B, and E, respectively, where all the variables result from a binary random variable sent through three independent channels, the secret key agreement is possible iff $I(X;Y|Z) > 0$.

[362] **061820**, **'On a Special Class of Broadcast Channels with Confidential Messages'**
M. van Dijk, IEEE Transactions on Information Theory, vol. 42 no. 2 pp. 712–714, Mar. 1997 , .
The author reinterprets Csisár and Körner's characterisation of noisy memoryless channels in terms of mutual information, and applies it to the wiretap channel. This enables him to prove that if the channels from the sender to the receiver and the eavesdropper are both symmetric, discrete and memoryless, then the secrecy capacity between the sender and receiver is precisely the difference in capacity between the channels to the receiver and the eavesdropper.

[363] **'Modeling the False Alarm and Missed Detection Rate for Electronic Watermarks'**
J.-P. Linnartz, T. Kalker, G. Depovere, in Aucsmith [369], pp. 329–343.
The authors present a model of the detection reliability of copyright marks as a function of energy, spatial correlation, cover image luminance variance and signal-to-noise ratio. With a white watermark, the signal-to-noise ratio (mar-to-content energy) is the only factor that influences the detection probability, but with other spectra we get some counterintuitive results; for example, a random DC component in the mark often aids its detection. Some experimental results are given which support the model.
`<http://diva.eecs.berkeley.edu/~linnartz/errate.ps.Z>`.

[364] **'Throwing more Light on Image Watermarks'**
J. R. Hernández, F. Pérez-González, in Aucsmith [369], pp. 191–207.
The authors give an information-theoretical analysis of watermarking systems. Imperceptibility, hiding process, detection process and some attacks (AWGN, linear filtering, resampling and cropping) are presented formally. A spread spectrum system is presented as a particular case of the general model.

[365] **'An Information-Theoretic Model for Steganography'**
C. Cachin, in Aucsmith [369], pp. 306–318.
The author uses the relative entropy (or discrimination) between the probability distributions of the cover-text P_C and of the stego-text P_S to define the security of the system: a stego-system is called perfectly ϵ-secure if $D(P_C||P_S) \leq \epsilon$. Based on this definition the author proposes two perfectly secure stego systems.

[366] **'Steganalysis and Game Equilibria'**
J. M. Ettinger, in Aucsmith [369], pp. 319–328.
A two-player, zero-sum, matrix game in introduced for modelling the contest between a data-hider and an attacker. The solution of the game depends on the permitted distortion and its value is the amount of information actually hidden.

[367] **'Modeling the security of Steganographic systems'**
J. Zöllner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, G. Wolf, in Aucsmith [369], pp. 344–354.
An information-theoretical model of steganography is introduced. It is shown that secure steganography is impossible when both cover and stego objects are known to the attacker. Uncertainty about the cover-object is introduced into the model to obtain better security.

[368] **'Information hiding: first international workshop'**
R. J. Anderson, Ed., vol. 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, May 1996. Springer-Verlag, Berlin, Germany. ISBN 3-540-61996-8.
This workshop on information hiding formed part of a six month research programme which was held in 1996 at the Isaac Newton Institute on Computer Security, Cryptography and Coding Theory.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[369] **'Information Hiding: Second International Workshop'**
D. Aucsmith, Ed., vol. 1525 of Lecture Notes in Computer Science, Portland, Oregon, U.S.A., 1998. Springer-Verlag, Berlin, Germany. ISBN 3-540-65386-4.

13 Patents

[370] **'Steganographic method and device'**
M. Cooperman, S. A. Moskowitz, U.S. Patent 5,613,004, Mar. 1995.

The authors detail a method for encoding a watermark into digital audio and how it can be used to establish ownership of copyrighted digital multimedia content. The marking technique embeds the watermark into the least significant bits of the Fourier transform of the sound. A pseudo-random mask tells which frequency band to modify. A set of cryptographic protocols based on this steganographic technique is then proposed; it involves the copyright owner, a publisher, a trusted authority and the consumer.

[371] **'Steganography methods employing embedded calibration data'**
G. B. Rhoads, U.S. Patent 5,636,292, June 1997.

[372] **'Simultaneous transmission of speech and data over an analog channel'**
R. D. Nash, W. C. Wong, U.S. Patent 4,512,013, Apr. 1985.

[373] **'Method and apparatus for data hiding in images'**
W. Bender, N. Morimoto, D. Gruhl, U.S. Patent 5,870,499, 17 Feb. 1999.

[374] **'Method and apparatus for echo data hiding in audio signals'**
W. Bender, D. Gruhl, N. Morimoto, U.S. Patent 5,893,067, 6 Apr. 1999.

[375] **'Security document system and method'**
R. B. Godlewski, R. D. Harris, M. J. Tinghitella, U.S. Patent 3,852,088, 3 Dec. 1974.
Provide an ink of a color that is highly reflective across the operating energy range of at least one group of copiers operating predominantly in the blue region. Other claims.

14 Other papers

[376] **'Covert Distributed processing with Computer Viruses'**
S. R. White, in Advances in Cryptology — Crypto '89, 1989, vol. 435 of Lecture Notes in Computer Science, pp. 616–619.
Viruses can be used to perform distributed processing without the knowledge or consent of the machine owners. The class of problems for which such processing might be useful is discussed, and includes keysearch; a virus which infected ten million machines might break a DES key in about three months.

[377] **'A short course in computer viruses'**
F. B. Cohen, Wiley, 2 edition, 1994. ISBN 0-471-00769-2.
Fred Cohen is uniquely qualified to write about computer viruses, having invented them twelve years ago as his PhD project. In addition to a brief history of the subject, including covert channel attacks on military secure Unix systems, he ranges from theoretical results on undecidability through to practical accounts of the latest virus and anti-virus techniques.

[378] **'Reflections on Trusting Trust'**
K. Thomson, Communications of the A.C.M., vol. 27 no. 8, Aug. 1984 , .
In his Turing award lecture, Ken Thomson shows that a Trojan horse can be hidden in a compiler; it inserts copies of itself every time either the compiler or the login program is compiled.

[379] **'The new Dutch passport'**
D. van Lingen, in van Renesse [401], pp. 67–73.
The author reviews all the optical and physical security features included in the new Dutch passport such as: special wefts, intaglios, optical variable inks, kinegrams, microtext, fugitive inks and special laminates.

[380] **034404**, **'Recursive mappings for computer virus'**
X. A. Li, J. H. Fu, Y. G. Song, H. Y. Yang, in Chinacrypt '94, Xidian, China, 11–15 Nov. 1994, pp. 279–286.

This paper builds on Adleman's suggested definition of computer viruses in terms of Gödel numberings, and suggests a recursive mapping definition. They show that programs exist which are viruses under their definition but not Adleman's and vice versa; and that for any virus, there exists a program which it cannot infect or injure.

[381] **043125**, **'The trustworthy digital camera: restoring credibility to the photographic image'**
G. L. Friedman, IEEE Transactions on Consumer Electronics, vol. 39 no. 4 pp. 905–910, Nov. 1993 , .
The author describes how to embed a signature capability in a digital camera for forensic applications. He suggests that a secure processor with signing keys be embedded in the camera at manufacture; the signature would secure not just the image, but also the time and data, light level, colour temperature, focusing distance and maybe even GPS location data. All this additional information would be held in a strip at the side of the picture.

[382] **054104**, **'Tamper Resistant Software: An Implementation'**
D. Aucsmith, in Anderson [402], pp. 317–333.
The author describes some techniques developed at Intel for making software difficult to debug without processor emulators or other specialised hardware analysis tools. The basic ideas are to have a number of interdependent modules that cooperate to generate threshold signatures, so that the secret key is never present all at once in memory or processed in a single operation; to customise the code to each installation by interleaving and obfuscating operations in varying ways; and to have the modules verify each others' integrity. Signatures of known debuggers and emulators are also detected, and with some processors integrity verification code can be locked in the cache.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[383] **054327**, **'Establishing Big Brother Using Covert Channel and Other Covert Techniques'**
Y. Desmedt, in Anderson [402], pp. 64–71.
The author discusses a number of ways in which covert technologies that are initially deployed for relatively mundane purposes, such as copyright protection, can end up being subverted to provide the means of surveillance. This problem could become progressively more serious as more and more everyday objects become endowed with some kind of intelligence and communications capability.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[384] **054407**, **'Oblivious Key Escrow'**
M. Blaze, in Anderson [402], pp. 335–343.
The author describes how key escrow could be performed using 'the net' as a highly reliable escrow server. For example, a secret key could be shared using a 500-out-of-5000 secret sharing scheme, so that it could still be recovered after the failure of 90% of network nodes. The sharing can be done with a new protocol technique called 'oblivious multicast', in which each share might end up in one out of a million possible nodes, with the sharer not knowing which. Access to the key would involve broadcast and thus surreptitious abuse of the escrow mechanism would be prevented.
`<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>`.

[385] **062326**, **'Verschlüsselungsverfahren – Eine Kurzübersicht'**
R. W. Gerling, Datenschutz und Datensicherheit, vol. 21 no. 4 pp. 197–201, Apr. 1997 , .

The author gives a background briefing on the technical issues behind the crypto policy debate, including basic crypto, key establishment protocols, steganography and network services.

[386] **062338**, **'Zur Notwendigkeit der Kryptographie'**
S. Kelm, K. P. Kossakowski, Datenschutz und Datensicherheit, vol. 21 no. 4 pp. 192–196, Apr. 1997 , .
The authors argue that strong cryptography is necessary for building trust in network applications and that its control by the state within constitutionally acceptable limits is unfeasible, because of the intrusiveness of measures needed to prevent criminals using double encryption or steganography.

[387] **062815**, **'Information-Theoretically Secure Secret-Key Agreement by NOT Authenticated Public Discussion'**
U. Maurer, in Advances in Cryptography – Eurocrypt '97, Konstanz, Germany, 11–15 May 1997, pp. 209–225, Springer-Verlag. ISBN 3-540-62975-0.
The author investigates the circumstances in which secret-key agreement can be secured against active adversaries. There are a number of negative results, such as that there can exist no unconditionally-secure public-key encryption system. However, it is possible to set up a secret in the wiretap channel provided that Eve's channel is noisier than Alice's and Bob's.

[388] **064343**, **'A History Of Computer Viruses'**
H. J. Highland, Computers and Security, vol. 16 no. 5 pp. 412–438, 1997 , .
This is a three-part article containing a history of computer viruses, an overview of five famous viruses and a discussion of macro viruses.

[389] **064345**, **'Procedures To Reduce The Computer Virus Threat'**
H. J. Highland, Computers and Security, vol. 16 no. 5 pp. 439–449, 1997 , .
This is a three-part article containing a history of computer viruses, an overview of five famous viruses and a discussion of macro viruses.

[390] **073818**, **'An Efficient Discrete Log Pseudo Random Generator'**
S. Patel, G. S. Sundaram, in 18th Annual International Cryptology Conference. 23–27 Aug. 1998, vol. 1462 of Lecture Notes in Computer Science, pp. 304–317, Springer-Verlag.
The authors show that discrete exponentiation modulo a prime p can hide $n - w(\log n)$ bits where $n = \lceil \log p \rceil$ and $p = 2q + 1$, where q is also a prime. They prove that any information about the $n - w(\log n)$ bits can be used to discover the discrete log of $g^s \bmod p$ where s has $w(\log n)$ bits. By setting the size of s by a constant c bits, a random number generator which produces $n-c$ bits per iteration is introduced.

[391] **073127**, **'Protecting VoD the Easier Way'**
C. Griwodz, O. Merkel, J. Dittmann, R. Steinmetz, [404], pp. 21–28.
The authors propose a system for protecting video over multicast via content corruption. With multicast all users receive the same information and it is not commercially feasible to restrict content access to a small group of receivers. It is suggested that the multicast server could broadcast corrupted data (and so useless) which could also be stored on cache servers. For decoding, users would have to receive reconstruction information via a unicast channel. The advantage is that the information needed for reconstruction is very small compared to the full video. Corruption is done by changing at random some bits in the stream making it undecodable; these errors are emphasised and spread thanks to the Huffman tables.

[392] **073569**, **'A Fast MPEG Video Encryption Algorithm'**
C. Shi, B. Bhargava, [404], pp. 81–88.
This is a variant of the one-time pad: the sign bit of the Huffman codes of the MPEG stream are XORed with an pseudo random string.

[393] **074108**, **'Search for effective document security by 'inventioneering"**
J. D. Brongers, in van Renesse [403], pp. 29–38.
The author argues that means to countermeasure counterfeiting must concentrate on posing new problems for counterfeiters and forgers, rather than concentrate on improvements of existing means. Several practical examples are given: carbon-based penetrating ink (against frauders who "washed" cheques printed on laser printers), CO_2 laser perforated cards, personalised OVDs (transgraving), offset ink hidden toner and micro laser engraving in screen offset printed artwork.

[394] **074113**, **'Evaluation security features in new design U.S. currency'**
S. E. Church, T. A. Ferguson, in van Renesse [403], pp. 8–20.
The authors review the main feature of the $100 note introduced in March 1996 and counterfeit of this note. They first characterise and quantify (quality and effectiveness) various counterfeits that have been generated. Then they analyse the counterfeiting trends to show the impact of the introduction of the new security features.

[395] **074125**, **'Secure Identification Documents via Pattern Recognition and Public Cryptography'**
L. O'Gorman, I. Ralinovich, IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 20 no. 10 pp. 1097–1102, Oct. 1998 , .
The authors use local and global features of photo (based on colour averaging) as base for a concise representation of the a photo for later use in a signature printed on a identification document. The authentication can be stand-alone or can use database.

[396] **074127**, **'Video Protection by Partial Content Corruption'**
C. Griwotz, in Dittmann et al. [405], pp. 37–39.
This is a short version of [391].

[397] **074148**, **'Watermarking in the Real World: An Application to DVD'**
M. L. Miller, I. J. Cox, J. A. Bloom, in Dittmann et al. [405], pp. 71–76.
The authors explain the rational behind the DVD security technology. They argue that watermarking was the easy part of the problem; system design was the most difficult: number of gates, cost, false positive alarm around 1 in 10^12.

[398] **074149**, **'Technology Approaches to Currency Security'**
J. C. Murphy, D. Dubbel, R. Benson, in van Renesse [403], pp. 21–28.
The authors list the security features used in the new $100 banknote and the parties involved in its design. They then focus their discussion on the concept of "selected tags," a mechanisms to automate or to simplify the dectection of counterfeit banknote. In particular they show how this can be achieved using photoacoustic effects or inks containing piezo-electric material.

[399] **074177**, **'Verifying versus falsifying banknotes'**
R. L. van Renesse, Optical Security and Counterfeit Deterrence Techniques II [403], pp. 71–85.
The author gives the result of a study of counterfeit banknotes. For each security feature, the author shows what makes it difficult to reproduce and whether it can be used as positive evidence (the presence of the feature is a strong indication of genuineness) or negative evidence (absence of the feature proves counterfeit). From the study it appears that, in general, banknotes are falsifiable in the sense that their genuineness cannot be readily confirmed by the inspection of a single security feature. Watermarks remain one of the best security features. It also appears that many features do not fully suffice for public inspection, as they require attentive observation and some expertise.

[400] **'Method for hiding information in lattice'**
D. H. Nyang, S. S. Song, Electronics Letters, vol. 34 no. 23 pp. 2226–2228, Nov. 1998

, .
This is an interactive challenge response identification protocol.

[401] **'Optical Security and Counterfeit Deterrence Techniques'**
R. L. van Renesse, Ed., vol. 2659, San Jose, California, U.S.A., Feb. 1996. The Society for Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIE), SPIE. ISBN 0-8194-2033-6, ISSN 0277-786X.

[402] **'Information hiding: first international workshop'**
R. J. Anderson, Ed., vol. 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, May 1996. Springer-Verlag, Berlin, Germany. ISBN 3-540-61996-8.
This workshop on information hiding formed part of a six month research programme which was held in 1996 at the Isaac Newton Institute on Computer Security, Cryptography and Coding Theory.
<http://www.springer.de/catalog/html-files/deutsch/comp/3540619968.html>.

[403] **'Optical Security and Counterfeit Deterrence Techniques II'**
R. L. van Renesse, Ed., vol. 3314, San Jose, California, U.S.A., 28–30 Jan. 1998. The Society for Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIE), SPIE. ISBN 0-8194-2556-7, ISSN 0277-786X.

[404] **'6th ACM International Multimedia Conference (ACM Multimedia'98)'**
ACM, Bristol, England, Sept. 1998. ISBN 1-58113-036-8.

[405] **'Multimedia and Security – Workshop at ACM Multimedia'98'**
J. Dittmann, P. Wohlmacher, P. Horster, R. Steinmetz, Eds., vol. 41 of GMD Report, Bristol, United Kingdom, Sept. 1998. ACM, GMD – Forschungszentrum Informationstechnik GmbH, Darmstadt, Germany.

15 Other bibliographies

- Additional references by Neil Johnson: <http://www.jjtc.com/Steganography/readings.htm>
- Index of Cryptography Papers Available Online by Bruce Schneier: <http://www.counterpane.com/biblio/>
- Publication of the University of Geneva (on digital watermarking): <http://cuiwww.unige.ch/~vision/Publications/watermarking_publications.html>
- biburlhttp://www.ee.umn.edu/groups/msp/subject/mmedia.html Publications of the University of Minnesota (multimedia applications of wavelets, including digital watermarking):
- Bibliography of Multimedia Authentication Research Papers by Ching-yung Lin: <http://www.ctr.columbia.edu/~cylin/auth/bibauth.html>
- Archive of papers on image watermarking, denoising & wavelets by Patrick Loo: <http://paddy.trin.cam.ac.uk/pl201/papers.html>
- Papers by Ron van Schyndel's et al. on watermarking: <http://www.physics.monash.edu.au/~ron/papers>
- Watermarking 3D objects by Ryutarou Ohbuchi: <http://www.kki.yamanashi.ac.jp/~ohbuchi/research/3dwmbib.html>